ATTACHMENT D–GDIT CONTRACT

COMMONWEALTH OF MASSACHUSETTS ~ STANDARD CONTRACT FORM

This form is jointly issued and published by the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) as the default contract for all Commonwealth Departments when another form is not prescribed by regulation or policy. Any changes to the official printed language of this form shall be void. Additional non-conflicting terms may be added by Attachment. Contractors may not require any additional agreements, engagement letters, contract forms or other additional terms as part of this Contract without prior Department approval. Click on hyperlinks for definitions, instructions and legal requirements that are incorporated by reference into this Contract. An electronic copy of this form is available at www.mass.gov/osc under Guidance For Vendors - Forms or www.mass.gov/osd under OSD Forms.

CONTRACTOR LEGAL NAME: **General Dynamics Information Technology, Inc.** (and d/b/a):	COMMONWEALTH DEPARTMENT NAME: **State 911 Department** MMARS Department Code: **EPS**
Legal Address: **(W-9, W-4,T&C): 77 "A" Street, Needham, MA 02494**	Business Mailing Address: **1380 Bay Street, Building C, Taunton, MA 02780**
Contract Manager: **Stephen Woodworth**	Billing Address (if different):
E-Mail: **Stephen.woodworth@gdit.com**	Contract Manager: **Tom Ashe**
Phone: **781-400-7460** Fax: **781-455-5100**	E-Mail: **Tom.Ashe@state.ma.us**
Contractor Vendor Code: **VC0000742753C**	Phone: **508-821-7203** Fax: **508-828-2585**
Vendor Code Address ID (e.g. "AD001"): **AD001** (Note: The Address Id Must be set up for EFT payments.)	MMARS Doc ID(s): **CT EPS 15GNDJNSTATE911400 2** 0 RFR/Procurement or Other ID Number: **State 911 14-002**

X NEW CONTRACT PROCUREMENT OR EXCEPTION TYPE: **(Check one option only)** __ Statewide Contract (OSD or an OSD-designated Department) __ Collective Purchase (Attach OSD approval, scope, budget) **X** Department Procurement (includes State or Federal grants 815 CMR 2.00) (Attach RFR and Response or other procurement supporting documentation) __ Emergency Contract (Attach justification for emergency, scope, budget) __ Contract Employee (Attach Employment Status Form, scope, budget) __ Legislative/Legal or Other: (Attach authorizing language/justification, scope and budget)	__ CONTRACT AMENDMENT Enter **Current Contract End Date** *Prior* to Amendment: _____, 20___. Enter **Amendment Amount:** $_____. (or "no change") AMENDMENT TYPE: **(Check one option only. Attach details of Amendment changes.)** __ Amendment to Scope or Budget (Attach updated scope and budget) __ Interim Contract (Attach justification for Interim Contract and updated scope/budget) __ Contract Employee (Attach any updates to scope or budget) __ Legislative/Legal or Other: (Attach authorizing language/justification and updated scope and budget)

The following COMMONWEALTH TERMS AND CONDITIONS (T&C) has been executed, filed with CTR and is incorporated by reference into this Contract.

X Commonwealth Terms and Conditions __ Commonwealth Terms and Conditions For Human and Social Services

COMPENSATION: (Check ONE option): The Department certifies that payments for authorized performance accepted in accordance with the terms of this Contract will be supported in the state accounting system by sufficient appropriations or other non-appropriated funds, subject to intercept for Commonwealth owed debts under 815 CMR 9.00.

X Rate Contract (No Maximum Obligation. Attach details of all rates, units, calculations, conditions or terms and any changes if rates or terms are being amended.)

__ Maximum Obligation Contract Enter Total Maximum Obligation for total duration of this Contract (or *new* Total if Contract is being amended). $_____.

PROMPT PAYMENT DISCOUNTS (PPD): Commonwealth payments are issued through EFT 45 days from invoice receipt. Contractors requesting accelerated payments must identify a PPD as follows: Payment issued within 10 days **1** % PPD; Payment issued within 15 days **0.5** % PPD; Payment issued within 20 days **0.25** % PPD; Payment issued within 30 days **0** % PPD. If PPD percentages are left blank, identify reason: __agree to standard 45 day cycle __ statutory/legal or Ready Payments (G.L. c. 29, § 23A); __ only initial payment (subsequent payments scheduled to support standard EFT 45 day payment cycle. See Prompt Pay Discounts Policy.)

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE or REASON FOR AMENDMENT: (Enter the Contract title, purpose, fiscal year(s) and a detailed description of the scope of performance or what is being amended for a Contract Amendment. Attach all supporting documentation and justifications.) **Contract is for the provision of Next Generation 911 Products and Services per the specifications and requirements of State 911 14-002 and the contractor's RFR response, inclusive of clarification letters dated July 14 and July 28, 2014.**

ANTICIPATED START DATE: (Complete ONE option only) The Department and Contractor certify for this Contract, or Contract Amendment, that Contract obligations:

X 1. may be incurred as of the Effective Date (latest signature date below) and no obligations have been incurred prior to the Effective Date.

__ 2. may be incurred as of _____, 20___, a date LATER than the Effective Date below and no obligations have been incurred prior to the Effective Date.

__ 3. were incurred as of _____, 20___, a date PRIOR to the Effective Date below, and the parties agree that payments for any obligations incurred prior to the Effective Date are authorized to be made either as settlement payments or as authorized reimbursement payments, and that the details and circumstances of all obligations under this Contract are attached and incorporated into this Contract. Acceptance of payments forever releases the Commonwealth from further claims related to these obligations.

CONTRACT END DATE: Contract performance shall terminate as of **8-3-19**, with no new obligations being incurred after this date unless the Contract is properly amended, provided that the terms of this Contract and performance expectations and obligations shall survive its termination for the purpose of resolving any claim or dispute, for completing any negotiated terms and warranties, to allow any close out or transition performance, reporting, invoicing or final payments, or during any lapse between amendments.

CERTIFICATIONS: Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified above, subject to any required approvals. The Contractor makes all certifications required under the attached Contractor Certifications (incorporated by reference if not attached hereto) under the pains and penalties of perjury, agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein according to the following hierarchy of document precedence, the applicable Commonwealth Terms and Conditions, this Standard Contract Form including the Instructions and Contractor Certifications, the Request for Response (RFR) or other solicitation, the Contractor's Response, and additional negotiated terms, provided that additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.

AUTHORIZING SIGNATURE FOR THE CONTRACTOR: X: _____. Date: 8/1/2014 (Signature and Date Must Be Handwritten At Time of Signature) Print Name: **Peter Bertocci** Print Title: **Sr. Director of Contracts**	AUTHORIZING SIGNATURE FOR THE COMMONWEALTH: X: _____. Date: 8/4/14 (Signature and Date Must Be Handwritten At Time of Signature) Print Name: **Frank Pozniak** Print Title: **Executive Director**

COMMONWEALTH OF MASSACHUSETTS ~ STANDARD CONTRACT FORM

This form is jointly issued and published by the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) as the default contract for all Commonwealth Departments when another form is not prescribed by regulation or policy. Any changes to the official printed language of this form shall be void. Additional non-conflicting terms may be added by Attachment. Contractors may not require any additional agreements, engagement letters, contract forms or other additional terms as part of this Contract without prior Department approval. Click on hyperlinks for definitions, instructions and legal requirements that are incorporated by reference into this Contract. An electronic copy of this form is available at www.mass.gov/osc under Guidance For Vendors - Forms or www.mass.gov/osd under OSD Forms.

CONTRACTOR LEGAL NAME: General Dynamics Information Technology, Inc. (and d/b/a):	**COMMONWEALTH DEPARTMENT NAME:** State 911 Department **MMARS Department Code:** EPS
Legal Address: (W-9, W-4,T&C): 77 "A" Street, Needham, MA 02494	**Business Mailing Address:** 1380 Bay Street, Building C, Taunton, MA 02780
Contract Manager: Stephen Woodworth	**Billing Address** (if different):
E-Mail: Stephen.woodworth@gdit.com	**Contract Manager:** Tom Ashe
Phone: 781-400-7460 **Fax:** 781-455-5100	**E-Mail:** Tom.Ashe@state.ma.us
Contractor Vendor Code: VC0000742753	**Phone:** 508-821-7203 **Fax:** 508-828-2585
Vendor Code Address ID (e.g. "AD001"): AD 001 (Note: The Address Id Must be set up for EFT payments.)	**MMARS Doc ID(s):** CT EPS 15GNDYNSTATE91114002 **RFR/Procurement or Other ID Number:** State 911 14-002

__ NEW CONTRACT

PROCUREMENT OR EXCEPTION TYPE: (Check one option only)

__ Statewide Contract (OSD or an OSD-designated Department)
__ Collective Purchase (Attach OSD approval, scope, budget)
__ Department Procurement (includes State or Federal grants 815 CMR 2.00) (Attach RFR and Response or other procurement supporting documentation)
__ Emergency Contract (Attach justification for emergency, scope, budget)
__ Contract Employee (Attach Employment Status Form, scope, budget)
__ Legislative/Legal or Other: (Attach authorizing language/justification, scope and budget)

X CONTRACT AMENDMENT

Enter Current Contract End Date *Prior* to Amendment: August 3, 2018
Enter Amendment Amount: $ "no change" (or "no change")

AMENDMENT TYPE: (Check one option only. Attach details of Amendment changes.)

X Amendment to Scope or Budget (Attach updated scope and budget)
__ Interim Contract (Attach justification for Interim Contract and updated scope/budget)
__ Contract Employee (Attach any updates to scope or budget)
__ Legislative/Legal or Other: (Attach authorizing language/justification and updated scope and budget)

The following COMMONWEALTH TERMS AND CONDITIONS (T&C) has been executed, filed with CTR and is incorporated by reference into this Contract.

X Commonwealth Terms and Conditions __ Commonwealth Terms and Conditions For Human and Social Services

COMPENSATION: (Check ONE option): The Department certifies that payments for authorized performance accepted in accordance with the terms of this Contract will be supported in the state accounting system by sufficient appropriations or other non-appropriated funds, subject to intercept for Commonwealth owed debts under 815 CMR 9.00.

X Rate Contract (No Maximum Obligation. Attach details of all rates, units, calculations, conditions or terms and any changes if rates or terms are being amended.)

__ Maximum Obligation Contract Enter Total Maximum Obligation for total duration of this Contract (or *new* Total if Contract is being amended). $ _____

PROMPT PAYMENT DISCOUNTS (PPD): Commonwealth payments are issued through EFT 45 days from invoice receipt. Contractors requesting accelerated payments must identify a PPD as follows: Payment issued within 10 days 1 % PPD; Payment issued within 15 days 0.5 % PPD; Payment issued within 20 days 0.25 % PPD; Payment issued within 30 days 0 % PPD. If PPD percentages are left blank, identify reason: __agree to standard 45 day cycle __ statutory/legal or Ready Payments (G.L. c. 29, § 23A); __ only initial payment (subsequent payments scheduled to support standard EFT 45 day payment cycle. See Prompt Pay Discounts Policy.)

BRIEF DESCRIPTION OF CONTRACT PERFORMANCE or REASON FOR AMENDMENT: (Enter the Contract title, purpose, fiscal year(s) and a detailed description of the scope of performance or what is being amended for a Contract Amendment. Attach all supporting documentation and justifications.) Contract amendment supersedes and replaces Attachment L- Project Schedule, Deliverables and Milestones and makes attendant changes in Retainage. All other rates, terms, and conditions remain in effect.

ANTICIPATED START DATE: (Complete ONE option only) The Department and Contractor certify for this Contract, or Contract Amendment, that Contract obligations:

X 1. may be incurred as of the Effective Date (latest signature date below) and no obligations have been incurred prior to the Effective Date.
__ 2. may be incurred as of _____, 20___, a date LATER than the Effective Date below and no obligations have been incurred prior to the Effective Date.
__ 3. were incurred as of _____, 20___, a date PRIOR to the Effective Date below, and the parties agree that payments for any obligations incurred prior to the Effective Date are authorized to be made either as settlement payments or as authorized reimbursement payments, and that the details and circumstances of all obligations under this Contract are attached and incorporated into this Contract. Acceptance of payments forever releases the Commonwealth from further claims related to these obligations.

CONTRACT END DATE: Contract performance shall terminate as of August 3, 2019, with no new obligations being incurred after this date unless the Contract is properly amended, provided that the terms of this Contract and performance expectations and obligations shall survive its termination for the purpose of resolving any claim or dispute, for completing any negotiated terms and warranties, to allow any close out or transition performance, reporting, invoicing or final payments, or during any lapse between amendments.

CERTIFICATIONS: Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract or Amendment shall be the latest date that this Contract or Amendment has been executed by an authorized signatory of the Contractor, the Department, or a later Contract or Amendment Start Date specified above, subject to any required approvals. The Contractor makes all certifications required under the attached Contractor Certifications (incorporated by reference if not attached hereto) under the pains and penalties of perjury, agrees to provide any required documentation upon request to support compliance, and agrees that all terms governing performance of this Contract and doing business in Massachusetts are attached or incorporated by reference herein according to the following hierarchy of document precedence, the applicable Commonwealth Terms and Conditions, this Standard Contract Form including the Instructions and Contractor Certifications, the Request for Response (RFR) or other solicitation, the Contractor's Response, and additional negotiated terms, provided that additional negotiated terms will take precedence over the relevant terms in the RFR and the Contractor's Response only if made using the process outlined in 801 CMR 21.07, incorporated herein, provided that any amended RFR or Response terms result in best value, lower costs, or a more cost effective Contract.

AUTHORIZING SIGNATURE FOR THE CONTRACTOR:
X: Stephen L Woodworth, Date: 2/26/15
(Signature and Date Must Be Handwritten At Time of Signature)
Print Name: Stephen L Woodworth
Print Title: Contracts Manager

AUTHORIZING SIGNATURE FOR THE COMMONWEALTH:
X: _____, Date: 2/27/15
(Signature and Date Must Be Handwritten At Time of Signature)
Print Name: Frank Poznlak
Print Title: Executive Director

Amendment to Contract for the Provision of
Next Generation 911 Products and Services
dated August 4, 2014 By and Between
The Commonwealth of Massachusetts State 911 Department
and General Dynamics Information Technology, Inc.

This Amendment is attached to and forms a part of the Contract for the provision of Next Generation 911 Products and Services dated August 4, 2014 ("Contract" or "Agreement") entered into by and between the Commonwealth of Massachusetts State 911 Department ("State 911 Department") and General Dynamics Information Technology, Inc. (collectively "Parties").

Amended Rates, Terms, and Conditions. The following revisions to the rates, terms, and conditions of the Contract shall be effective immediately upon the Effective Date:

1. The provisions of paragraph one (1) of Section 8.14.4 Retainage are hereby superseded and replaced by the following language:

The State 911 Department will retain ten (10) percent of the total amount due to the contractor on each invoice for each Deliverable in Milestone Categories 1, 2, and 3. The State 911 Department will retain these amounts whether or not the contractor's performance is timely or the deliverable has met all of the State 911 Department's requirements for acceptance. The State 911 Department will release this ten (10) percent to the contractor if Milestone 3 is completed on or before June 5, 2015, and the lab staging, pre-installation test and checkout of the first PSAP selected for cutover in Milestone 4.1 commences on or before April 15, 2015. If either Milestone 3 is not completed on or before June 5, 2015, or the lab staging, pre-installation test and checkout of the first PSAP selected for cutover in Milestone 4.1 does not commence on or before April 15, 2015, the amount retained shall be forfeited to the Commonwealth, unless the State 911 Department elects, in its sole discretion, to waive such forfeiture.

2. Attachment L- Project Schedule, Deliverables, and Milestones is hereby superseded and replaced by Amended Attachment L- Project Schedule, Deliverables, and Milestones attached hereto and made a part hereof.

All of the other rates, terms and conditions of the Contract remain in full force and effect except as expressly amended hereby.

Amended Attachment L- Project Schedule, Deliverables, and Milestones

Milestone 1	System Design and Test Plan Development		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
1.1	**System Design**		
1.1.1	Develop and Submit to the State 911 Department System Design and Technical Documents	Detailed System Design Documents	Within sixty (60) days of contract award
1.1.2	Develop and Submit to the State 911 Department Detailed Network Design and Technical Documents	Detailed Network Design and Technical Documents	Within sixty (60) days of contract award
1.1.3	Develop and Submit to the State 911 Department Data Center Assessment, System Design and Technical Documents	Data Center Assessment, System Design and Technical Documents	Within thirty (30) days of contract award
1.1.4	Develop and Submit to the State 911 Department Detailed Security Plan	Detailed Security Plan	Within sixty (60) days of contract award
1.1.5	Develop and Submit to the State 911 Department a NOC/Help Desk Operational Manual	NOC/Help Desk Operations Manual	Within sixty (60) days of contract award
1.2	**Test Plan Development**		
1.2.1	Develop and Submit to the State 911 Department System Test Plan, (including Network Test Plan), Test Criteria, Test Cases and Scenarios, and Test Reports for each functional element of the system	System Test Plan (including Network Test Plan), Test Criteria, Test Cases and Scenarios, and Test Reports	9/12/2014
1.2.2	Develop and Submit to the State 911 Department Test Plan, Test Criteria, Test Cases and Scenarios, and Test Reports for GIS Data, Database, and LIS server function, including initial data loading validation, data normalization and load testing	GIS Data, Database, and LIS Server Test Plan, Test Criteria, Test Cases and Scenarios, Test Reports	9/12/2014

1.2.3	Develop and Submit to the State 911 Department Data Center Test Plan, Test Criteria, Test Cases and Scenarios, and Test Reports, for each data center	Data Center Test Plan, Test Criteria, Test Cases and Scenarios, Test Reports for each data center	9/12/2014
1.2.4	Develop and Submit to the State 911 Department NOC and Monitoring Test Plan, Tests Cases and Scenarios, Test Reports, and document how the system automatically generates trouble tickets and alarming and alerting functions	NOC and Monitoring Test Plan, Test Criteria, Test Cases and Test Scenarios, Test Reports	9/12/2014
1.2.5	Develop and Submit to the State 911 Department Security Test Plan and Test Criteria	Security Test Plan and Security Test Criteria	9/12/2014
1.2.6	Develop and Submit to the State 911 Department Test Schedule	Test Schedule	9/12/2014
		MILESTONE DUE	**October 3, 2014**

Milestone 2	**Laboratory Trial and Testing**		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
2.1	**Laboratory Trial and Testing Setup**		
2.1.1	Establish Laboratory Staging and Trial Testing Plan	Comprehensive Laboratory Staging and Trial Testing Plan	2/13/15
2.1.2	Install and Configure Test Equipment, Applications and Appliances and CPE using simulated equipment	Documentation that Test Equipment, Applications and Appliances, and CPE Installed and Prepared for Testing	2/18/15
2.2	**Laboratory Testing**		
2.2.1	Implement System Test Plan and Correct/Retest as necessary until Test Passed	Final Test Results Report	3/19/15
2.2.2	Implement GIS, Database, and LIS Server Test Plan and Correct/Retest	GIS, Database, and LIS Server Test Results	3/19/15

Milestone 2	Laboratory Trial and Testing		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
	as necessary until Test Passed	Report	
2.2.3	Implement NOC and Monitoring Test Plan and Correct/Retest as necessary until Test Passed and NOC processes and procedures refined to reflect results	NOC and Monitoring Test Results Report Updated Documentation	3/19/15
2.2.4	Implement Security Test Plan	Security Test Results Report	3/19/15
2.2.5	Event Recording Review and Refinement	Event Recording Results Report demonstrating operational functionality of Event Recording	3/19/15
2.2.6	Lab Testing Review and adjust any documentation from design phase based on Lab Testing Results	Final Test Acceptance	3/19/15
2.3	**Change Management Protocol Development**		
2.3.1	Develop and Submit to the State 911 Department Change Management Plan for hardware changes, software updates, software upgrade testing plan, determine change management team, inventory updates and documentation updates.	Change Management Plan	9/2/2014
2.4	**Finalize Network Design and Deployment Plans**		
2.4.1	Revise, Finalize, and Submit to the State 911 Department Network Design based on test results	Final Network Design Document	3/19/15
2.4.2	Revise, Finalize, and Submit to the State 911 Department Data Center Deployment Plan, and PSAP Deployment Plan based on test results, Deployment Schedule for data centers and PSAPs submitted, planning complete, data centers	Final Data Center and PSAP Deployment Plan	3/19/15

Milestone 2	Laboratory Trial and Testing		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
	prepared for commencement of pilot PSAP deployment, ordering schedule finalized		
2.5	**Training Plan Development**		
2.5.1	Develop Training Plan and Training Materials working with State Department	Training Plan and Training Materials	3/19/15
2.5.2	Develop Mobile Training Solution working with State 911 Department	Mobile Training Solution Documentation and Demonstration	3/19/15
2.5.3	Develop PSAP Pilot Deployment Training Schedule working with State 911 Department	Pilot PSAP Deployment Training Schedule	3/19/15
2.6	**Pilot Deployment Documentation and Processes**		
2.6.1	Develop and Submit to the State 911 Department Pilot PSAP Deployment Plan, Pilot PSAP Deployment Documentation (including Scheduling, Procurement, Installation, Quality Assurance and Work Order Documentation)	Pilot PSAP Deployment Plan and Pilot PSAP Deployment Documentation	3/19/15
2.6.2	In conjunction with State 911 Department, Develop and Deliver technical Training Plan and Materials to State 911 Department Systems staff and Develop and Deliver Training to State 911 Department Systems Staff on solution, read-only access to the Help Desk, and Monitoring systems	Training Plan and Materials and Certification of Training for State 911 Department Systems Staff	3/19/15
		MILESTONE DUE DATE	**March 19, 2015**

Milestone 3	Data Center Installations and Pilot Deployment Note: Only (2) position PSAPs may be used for the Pilot Deployment		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
3.1	**Data Center Installations**		
3.1.1	Install all equipment, applications and appliances, and software at Data Centers for Pilot Deployment	Equipment, Applications and Appliances, and Software Installed in Data Centers	4/2/2015
3.1.2	Implement Data Center Test Plans (including Stress Test Plan, Data Center Failover Test, including routing failover, physical plant failover, security, application failover, routing, and call distribution	Test Results Reports for all Data Center Test Plans	3/27/2015
3.1.3	Working with EOPSS and State 911 Department, develop Data Center Policies and Procedures for facilities, access procedures, security, notification and escalation processes	Data Center Policy and Procedures	4/29/2015
3.1.4	Review discussions, meetings and modifications as needed resulting from testing and data centers approved by the State 911 Department to be operational	Test Results, Acceptance Report, Site Acceptance Package for each Data Center	4/29/2015
3.2	**Training Center Installation**		
3.2.1	Install all equipment and CPE at Training Centers and connect Training Centers to Data Centers	State 911 Department Training Centers Operational Test Results, Acceptance Report, and Acceptance Package for each Training Center	4/29/15

3.3	**PSAP Pilot Deployment**		
3.3.1	Prepare Six (6) Pilot PSAPs per PSAP Pilot Deployment Plan approved by State 911 Department	Site Cutover Project Plan, Site Survey Form, Staging Test Results for each Pilot PSAP	4/2/2015
3.3.2	Cutover of Six (6) Pilot PSAPs in Pilot Deployment	Cutover Test Results, Post-Cutover Test Results, Cutover Acceptance Report, Site Cutover Acceptance Package for each Pilot Site	6/5/2015
		MILESTONE DUE DATE	**June 5, 2015**

Milestone 4	**PSAP Deployment** **Note: This Milestone includes the Mobile PSAP and from Attachment G - Boston Fire, Springfield Fire and Worcester Fire**		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
4.1	Cutover of 20 PSAPs	Cutover Acceptance Report for 20 PSAPs	August 17, 2015
4.2	Cutover of 30 PSAPs	Cutover Acceptance Report for 30PSAPs	October 16, 2015
4.3	Cutover of 34 PSAPs	Cutover Acceptance Report for 34 PSAPs	December 17, 2015
4.4	Cutover of 34 PSAPs	Cutover Acceptance Report for 34 PSAPs	February 16, 2016
4.5	Cutover of 28 PSAPs	Cutover Acceptance Report for 28 PSAPs	April 17, 2016
4.6	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	June 15, 2016
4.7	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	June 22, 2016

Milestone 4	PSAP Deployment Note: This Milestone includes the Mobile PSAP and from Attachment G - Boston Fire, Springfield Fire and Worcester Fire		
Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
4.8	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	June 30, 2016
		MILESTONE DUE DATE	June 30, 2016

Proposal for:

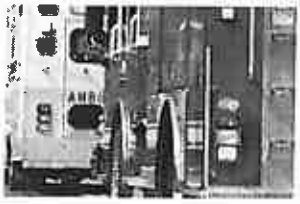
Next Generation 9-1-1 Emergency Communications System

RFR ID: State 911 14-002

May 23, 2014

Technical Response



Submitted to:

Karen Robitaille
State 911 Department
1380 Bay Street, Building C
Taunton, MA 02780

E-mail: Karen.Robitaille@state.ma.us

Submitted by:

GENERAL DYNAMICS
Information Technology

77 "A" Street
Needham, MA 02494-2806
www.gdit.com

Table of Contents

List of Tables

List of Figures

Section 1 – DEFINITIONS

1.1. ACRONYMS

Acronym	Definition
AAA	Authorization and Accounting
ACD	Automatic Call Distribution
ACE	American Council on Education
ACU	Audio Control Unit
AD	Active Directory
ADCS	Air Defense Communications Service
ADDIE	Analysis Design Development Implementation and Evaluation
AF	Air Force
AFNet	Air Force Network
AIU	Audio Interface Unit
AK	Alaska
ALI	Automatic Location Identification
ALMR	Alaska Land Mobile Radio
ANI	Automatic Number Identification
AP	Answering Positions
APCO	Association of Public-Safety Communications Officials
API	Application Programming Interface
APL	Approved Products List
ASA	Adaptive Security Appliance [Cisco]
ASCII	American Standard Code for Information Interchange
ASR	Aggregation Services Router
AT/IT	Adaptive Technology / Information Technology
ATA	Analog Telephone Adapters
ATP	Authorization to Proceed
ATS	Automatic Transfer Switch
AV	Audio Visual
AVL	Automatic Vehicle Location
B2BUA	Back to Back User Agent
BBA	Bachelor of Business Administration
BCF	Border Control Function

Acronym	Definition
BCI	Bureau of Criminal Identification
BGP	Border Gateway Protocol
BLII	Base Level Information Infrastructure
BOM	Bill of Materials
BRT	Business Recovery Team
BS	Bachelor of
BSEE	Bachelor of Science in Electrical Engineering
BTU	British Thermal Unit
C&A	Certification and Accreditation
CA	Certificate Authority
CAD	Computer-Aided Dispatch
CAIRS	Configuration Accounting Information Retrieval System
CAMA	Centralized Automatic Message Accounting
CAP	Common Alerting Protocol
CBCP	Contingency and Business Continuity Plans
CBQoS	Class Based Quality of Service
CBR	Constant Bit Rate
CCB	Configuration Control Board
CCP	Change Control Process
CCR	Central Contractor Registration
CD	Compact Disc
CDG	Course Description Guide
CDMA	Code Division Multiple Access
CDR	Call Detail Records
CDRW	Compact Disc Rewriteable
CDSE	Center for Development of Security Excellence
CE	Customer Edge
CEO	Chief Executive Officer
CER	Customer Edge Router
CFI	Commercially Furnished Information
CIA	Confidentiality Integrity and Availability
CIDB	Call Information Database
CIM	Critical Incident Management
CJI	Criminal Justice Information

Acronym	Definition
CJIS	Criminal Justice Information Services
CLE	Collaborative Learning Environment
CLEC	Competitive Local Exchange Carrier
CLID	Calling Line ID
CLIN	Contract Line Item Number
CLP	Competitive Local Provider
CM	Configuration Management
CMDB	Configuration Management Database
CME	CallManager Express
CMMI	Capability Maturity Model Integration
CMS	Configuration Management System
CO	Colorado
CONOPS	Concept of Operations
CONUS	Continental United States
COR	Class of Restriction, or Contracting Officer's Representative
COTS	Commercial Off-the-Shelf
CPARS	Contractor Performance Assessment Reporting System
CPE	Customer Premises Equipment
CPF	Common Process Framework
CPN	Calling Party Number
CPU	Central Processing Unit
CRAH	Computer Room Air Handler
CRM	Cluster Resource Manager
CSA	Cyber Situational Awareness
CSR	Certificate Signing Request
CSRIC	Communications Security Reliability and Interoperability Council
CTCAD	Counter Terrorism Components of Academy Development
CTO	Chief Technology Officer
CUCM	Cisco Unified Communications Manager
CWBS	Contractor Work Breakdown Structure
D&B	Dun Bradstreet
DAT	Distributing Agent
DAU	Defense Acquisition University
DCAA	Defense Contract Audit Agency

Acronym	Definition
DCMA	Defense Contract Management Agency
DCO	Defense Connect Online
DDL	Data Definition Language
DDM	Designated Defensive Marksman
DDoS	Distributed Denial of Service
DDTi	Digital Data Technologies, Inc.
DECC	Defense Enterprise Computing Center
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DLA	Defense Logistics Agency
DLC	Digital Loop Carriers
DLR	Digital Logging Recorder
DLSS	Depot Level Software Support
DMZ	Demilitarized Zone (perimeter network)
DN	Directory Number
DNS	Domain Name System
DO	Delivery Order
DoD	Department of Defense
DOE	Department of Energy
DOL	Department of Labor
DoS	Denial of Service
DRP	Disaster Recovery Plan
DRT	Disaster Recovery Team
DSCP	Differentiated Services Code Point
DSLAM	Digital Subscriber Line Access Multiplexers
DSN	Defense Switched Network
DSS	Defense Security Services
DTMF	Dual Tone Multi Frequency
DVR	Digital Video Recorder
DWDM	Dense Wavelength Division Multiplexing
E9-1-1	Enhanced 9-1-1
E&M	Ear and Mouth

Acronym	Definition
EAC	Estimate at Completion
EAL4	Evaluation Assurance Level 4
EBGP	External Border Gateway Protocol
ECP	Engineering Change Proposal
ECR	End of Course Report
ECRF	Emergency Call Routing Function
ECW	Emergency CallWorks
EF&I	Engineer, Furnish, and Install
EFI&T	Engineer, Furnish, Install, and Test
EFIT&C	Engineer, Furnish, Install, Test, and Cutover
EIA	Electronic Industries Alliance
EITC	Enterprise IT Center
EMS	Emergency Management System, or Element Management Systems
ENP	Emergency Number Professional
EOCC	Emergency Operations Command Center
EOPD	East Orange Police Department
EOPSS	Executive Office of Public Safety and Security
ePO	ePolicy Orchestrator [McAfee]
EPSS	Electronic Performance Support Systems
ERC	Emergency Response Communications
ERT	Emergency Response Team
ESD	Electrostatic Discharge
ESInet	Emergency Services IP Network
ESM	Enterprise Spend Management
ESN	Emergency Service Number
ESP	Encapsulating Security Payload
ESRK	Emergency Service Routing Key
ESRP	Emergency Services Routing Proxy
ESZ	Emergency Service Zones
ETA	Estimated Time of Arrival
ETL	Extract Translate and Load
EVCS	Enterprise Voice Consolidation System
EVMS	Earned Value Management System
FAA	Federal Aviation Administration

Acronym	Definition
FAS	Finance and Accounting System
FAVES	FAA Administrative Voice Enterprise Services
FBI	Federal Bureau of Investigation
FCAPS	Fault Configuration Accounting Performance Security
FCC	Federal Communications Commission
FE	Functional Element
FGDC	Federal Geographic Data Committee
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTE	Full-Time Equivalent
FTP	File Transfer Protocol
FTS	Federal Telecommunications System
GB	Gigabyte
GDAIS	General Dynamics Advanced Information Systems
GDC4S	General Dynamics C4 Systems
GDIT	General Dynamics Information Technology
GFE	Government Furnished Equipment
GFI	Government-Furnished Information
GFM	Government Furnished Material
GIS	Geographical Information System
GPIOM	General Purpose I/O Module
GPO	Group Policy Object
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSA	General Services Administration
GTBM	Gold Type Business Machines
GUI	Graphical User Interface
HA	High Availability
HCO	Hearing Carry Over
HELD	HTTP Enabled Location Delivery
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HN	Hostage Negotiation
HSRP	Hot Standby Router Protocol

Acronym	Definition
HVAC	Heating Ventilation and Air Conditioning
I/O	Input/Output
IA	In Accordance
ICE	Industry Collaboration Event
iCERT	Industry Council for Emergency Response Technologies
ICMP	Internet Control Message Protocol
IDIQ	Indefinite Delivery, Indefinite Quantity
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IECS	Integrated Emergency Communications System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIS	Information Services
IKE	IPsec Key Exchange
IL	Illinois
ILEC	Incumbent Local Exchange Carrier
ILT	Interdisciplinary Learning and Teaching
IMS	Integrated Master Schedule
IO	Interoperability
IOS	Internetwork Operating System
IP	Internet Protocol
IPA	Integrated Pictometry Analytics
IPAM	IP Address Management
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
IPsec	IP Security
IPSS	Integrated Performance Support Systems
IPT	IP Telephony
IPV6	Internet Protocol Version 6
IRIG	Inter Range Instrumentation Group
IRR	Instant Recall Recording
IRS	Internal Revenue Service
IS&T	Information Systems and Technology
ISDN	Integrated Services for Digital Network

Acronym	Definition
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISR	Integrated Services Router
ISUP	Integrated Services Digital Network User Part
IT	Is Telecommunications
ITA	Interdicting Terrorist Activities
ITAR/EAR	International Traffic in Arms Regulations / Export Administration Regulations
ITD	Information Technology Division
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
IVR	Interactive Voice Response
IWS	Intelligent Workstation
JACE	Java Application Control Engine
JBER	Joint Base Elmendorf Richardson
JCPD	Jersey City Police Department
JIT	Just in Time
JITC	Joint Interoperability Test Command
JRE	Java Runtime Environment
KPI	Key Performance Indicators
KVA	Kilovolt-Ampere
KVM	Keyboard Video Mouse
LAN	Local Area Network
LATA	Local Access Transport Area
LBI	Long Beach Island
LBRS	Location Based Response System
LCD	Liquid-Crystal Display
LCM	Life Cycle Maintenance
LCOE	Learning Center of Excellence
LDAP	Lightweight Directory Access Protocol
LDB	Location Database
LEAA	Law Enforcement Advanced Applications
LEC	Local Exchange Carrier
LED	Law Enforcement Desk
LI	Lawful Intercept

Acronym	Definition
LIF	Location Interface Function
LIS	Location Information Service
LLC	Limited Liability Company
LLQ	Low Latency Queuing
LMR	Land Mobile Radio
LMS	Learning Management System
LNG	Legacy Network Gateway
LO	Location Object
LoST	Location-to-Service Translation
LPG	Legacy PSAP Gateway
LSI	Large Systems Integrator
LSRG	Legacy Selective Router Gateway
LSS	Lean Six Sigma
LTE	Long Term Evolution
LVF	Location Validation Function
MA	Massachusetts
MAC	Moves, Adds, and Changes
MAST	Medical and Science Technology
MBA	Master of Business Administration
MBE	Minority Business Enterprise
MBI	Massachusetts Broadband Initiative
MCLB	Marine Corps Logistics Base
MD	Meade
MEC	Multi-chassis Etherchannel
MF	Multi-Frequency
MFS	Multi-Function Switch
MG	Media Gateways
MHz	Megahertz
MILDEP	Military Departments
MIS	Management Information System
MLTS	Multi Line Telephone System
MMS	Multimedia Messaging Service
MOP	Method of Procedure
MOS	Mean Opinion Score

Acronym	Definition
MPC	Mobile Positioning Center
MPLS	Multi-Protocol Label Switching
MSAG	Master Street Address Guide
MSRP	Message Session Relay Protocol
MTMP	Major Command Telephone Modernization Program
MWR	Morale Welfare and Recreation
N/A	Non-Disclosure Agreement
NAICS	North American Industry Classification System
NALF	Naval Auxiliary Landing Field
NAPT	Network Address and Port Translation
NAPTR	Name Authority Pointer
NAS	Naval Air Station
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NC	North Carolina
NCM	Network Configuration Manager
NDA	Non-Disclosure Agreements
NDRSMP	National Distress and Response System Modernization Project
NEBS	Network Equipment Building Systems
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NENA	National Emergency Number Association
NETC	Naval Education and Training Command
NETCENTS	Network Centric Systems
NETPDTC	Naval Education and Training Professional Development and Technology Center
NG	Next Generation
NG9-1-1	Next Generation 9-1-1
NH	New Hampshire
NIDS	Network Intrusion Detection System
NIF	Network Interface Function
NIST	National Institute of Standards and Technology
NJ	New Jersey
NKO	Navy Knowledge Online

Acronym	Definition
NLS	Nearline Disk Storage
NMS	Network Management System
NNI	Network to Network Interface
NOC	Network Operations Centers
NORAD	North American Aerospace Defense Command
NPM	Network Performance Monitor
NPSTC	National Public Safety Telecommunications Council
NSOC	Network and Security Operations Center
NTA	NetFlow Traffic Analyzer
NTP	Network Time Protocol
NTPS	NETPDTC) Training Products and Support
NY	New York
NYC	New York City
O&M	Operations and Maintenance
OCI	Organizational Conflict of Interest
OCONUS	Outside the Continental United States
OEC	Office of Emergency Communications
OEM	Original Equipment Manufacturer
OF	Opportunities FORMAT
O-FPA	Oracle Fan Pack Assembly
OMR	Optimized Media Routing
ONS	Optical Network Systems
OOS	Out of Scope
OPM	Office of Personnel Management
OS	Operating System
OSP	Outside Plant
OSS	Operations Support System
OTIS	Office of Technology and Information Services
P&L	Profit and Loss
PACAF	Pacific Air Force
PARRIS	Police Automated Radio Records Information System
PAST	Preventing Attacks on Soft Targets
PBX	Private Branch Exchange
PC	Personal Computer

Acronym	Definition
PCI	Payment Card Industry
PDF	Portable Document Format (Adobe]
PDU	Power Distribution Units
PE	Provider Edge
PEP	Policy Enforcement Point
PIDF-LO	Presence Information Data Format Location Object
PIF	Protocol Interworking Function
PITCO	Pre Installation Testing Check Out
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Project Manager
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Program Management Office
PMP	Project Management Professional
PNL	Protection of National Leadership
PO	Purchase Order
POA&M	Plan of Action and Milestones
POC	Point of Contact
POI	Program of Instruction
POP	Point of Presence
PRF	Policy Routing Function
PRI	Primary Rate Interface
PRR	Policy Routing Rules
PS/ALI	Private Switch Automatic Location Information
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTABRS	Preventing Terrorist Attacks on Bus and Rail Systems
PTAC	Procurement Technical Assistance Center
PTZ	Pan Tilt Zoom
PWS	Performance Work Statement
Q&A	Question and Answer
QA	Quality Assurance
QC	Quality Control

Acronym	Definition
QCP	Quality Control Plan
QEHS	Quality, Environmental, Health, and Safety
QMP	Quality Management Program
QMS	Quality Management System
QoS	Quality of Service
QSP	Quality Service Provider
RADIUS	Remote Authentication Dial in User Service
RCS	Rich Communication Services
RDP	Remote Desktop Protocol
REA	Request for Equitable Adjustment
RECC	Regional Emergency Communication Center
RFC	Request for Comments
RFP	Request for Proposal
RFR	Request for Response
RMB	Risk Management Board
RMS	Records Management System
ROADM	Reconfigurable Optical Add-Drop Multiplexer
ROI	Return on Investment
RSC	Remote Switching Center
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
RTS	Real Time Services
RU	Rack Unit
SALI	Stand-Alone ALI
SAM	Server and Applications Monitor
SB	Small Business
SBA	Small Business Administration
SBC	Session Border Controllers
SBLO	Small Business Liaison Officer
SBP	Small Business Program
SD	South Dakota
SDB	Small Disadvantaged Business
SDLC	System Development Life Cycle
SDO	Supplier Diversity Objectives

Acronym	Definition
SDP	Service Delivery Platform
SDVOBE	Service Disabled Veteran Owned Business Enterprises
SDVOSB	Service Disabled Veteran Owned Business
SI	Systems Integrator
SIE	Systems Integration Environment
SIEM	Security Information and Event Management
SIF	Signaling Information Field
SIP	Session Initiation Protocol
SIPREC	Session Recording Protocol
SLA	Service Level Agreements
SME	Subject Matter Experts
SMEO	Small End Office
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SNS	Satellite Network Solutions
SOC	Security Operations Centers
SOI	Service Order Input
SONET	Synchronous Optical Networking
SOWMBA	State Office for Minority and Women Business Assistance
SPoC	Single Point of Contact
SQL	Structured Query Language
SR	Selective Router
SRC	Session Recording Client
SRD	System Reference Document
SRTP	Secure Real-time Transport Protocol
SS7	Signaling System 7
SSH	Secure Shell
SSL	Secure Sockets Layer
STS	Static Switch
TACACS	Terminal Access Controller Access Control System
TB	Terabyte
TBD	To Be Determined
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol

Acronym	Definition
TCS	Telecommunication Systems, Inc.
TDD	Telecommunications Device for the Deaf
TDM	Traffic Demands
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TMN	Telecommunication Management Network
TN	Telephone Number
TNOM	Telecommunications Network Operations Managers
ToS	Type of Service
TPSS	Training and Performance Support System
TST	Tactical Support Team
TTY	Text Telephone
TX	Texas
UC	Unified Communications
UCAPL	Unified Capabilities Approved Product List
UCR	Unified Communications Requirements
UDP	User Datagram Protocol
UK	United Kingdom
UL	Underwriters Laboratories
UNDP	United Nations Development Program
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USAF	United States Air Force
USAFE	United States Air Forces in Europe
USB	Universal Serial Bus
USCG	United States Coast Guard
USM	Unified Security Management
USMC	United States Marine Corps
USNG	United States national Guard
USNORTHCOM	United States Northern Command
USPS	United States Postal Service
USTDA	United States Trade and Development Agency

Acronym	Definition
UT	Utah
VA	United States Department of Veterans Affairs, or Virginia
VBA	Veterans Benefits Administration
VCO	Voice Carry Over
VDI	Virtual Desktop Interfaces
VHA	Veterans Health Administration
VIPP	Very Important Person Protection
VIS	Vital Infrastructure Security
VLAN	Virtual Local Area Networks
VM	Virtualization Manager
VoIP	Voice over Internet Protocol
VOSB	Veteran-Owned Small Business
VP	Vice President
VPN	Virtual Private Network
VPO	Virtual Program Office
VRRP	Virtual Router Redundancy Protocol
VSR	Veterans Service Representatives
VSS	Virtual Switching Systems
VVoIP	Voice and Video over Internet Protocol
WA	Washington
WACS	Wire and Cable Services
WAN	Wide Area Network
WANSS	Wide Area Network Soft Switches
WBE	Women-Owned Business Enterprise
WBS	Work Breakdown Structure
WBT	Web Based Training
WDS	Windows Deployment Services
WHD	Web Help Desk
WI	Wisconsin
WIDTS	Worldwide Integrated Digital Telecommunication System
WMI	Web Management Interface
WOSB	
WPF	Windows Presentation Foundation
WSBE	Women Business Enterprises

Acronym	Definition
WSMR	White Sands Missile Range
WSPD	Winston Salem Police Department
WSUS	Windows Server Update Services
XML	Extensible Markup Language

Section 2 – DESCRIPTION OR PURPOSE OF THIS PROCUREMENT

The State 911 Department is responsible for coordinating, administering, and implementing enhanced 911 services and the enhanced 911 systems throughout Massachusetts to ensure a consistent statewide approach for enhanced 911 services. The State 911 Department seeks to contract with a qualified contractor or contractors to provide and operate a Next Generation 911 emergency communications system in Massachusetts. The State 911 Department seeks to procure the services of such contractor or contractors to design equip, install, operate, monitor, maintain, train, and support a Next Generation 911 system throughout the Commonwealth in a turnkey fashion.

The Commonwealth of Massachusetts, through the State 911 Department, invites vendors of Next Generation 911 services, appliances, products, and software to respond to this Request for Response.

The Commonwealth does not seek to procure GIS data through this RFR. Bidders shall not bid on the provision of GIS data, and cost proposals shall NOT include pricing for the provision of GIS data.

General Dynamics Information Technology (GDIT) complies with the RFR specification.

Section 3 – ACQUISITION METHOD TO BE USED FOR THIS CONTRACT

The acquisition method for this contract is fee for service. This contract has a durable commodities component in addition to the services. It is the State 911 Department's intent to take ownership of all durable commodities furnished under this contract, whether through an outright purchase or a tax-exempt lease purchase.

This contract will be a rate contract.

The contract will not have a maximum obligation amount. The total costs per unit shall be itemized according to Attachment E- Cost Tables.

The State 911 Department reserves the right to procure any goods and services through a procurement vehicle other than this RFR if to do so would result in the best value in fulfilling the contract, or any renewal thereof. The contractor may be required to evaluate such goods and services to ensure compatibility with the system.

GDIT complies with the RFR specification. GDIT is proposing to perform as prime contractor for the Next Generation 9-1-1 (NG9-1-1) emergency telecommunications system and will assume full responsibility for the aggregation of systems and components for the MA NG9-1-1 Emergency Communications System.

Section 4 – REQUEST FOR SINGLE OR MULTIPLE CONTRACTORS

The State 911 Department has a preference for the award of one (1) contract to a prime contractor who shall assume full responsibility for the aggregate of systems and components for the Next Generation 911 emergency telecommunications system (except the geographic information systems data that will be supplied by the Commonwealth), whether or not the goods and/or services are manufactured or produced by the prime contractor.

However, this RFR is not limited to bidders that propose to act as a prime contractor, and the State 911 Department reserves the right to accept bids and award contracts for components of the system as defined within this RFR. Bidders that provide discrete components that would comprise some portion of a Next Generation 911 emergency telecommunications system are permitted to submit a response.

GDIT complies with the RFR specification. GDIT is proposing to perform as prime contractor for the NG9-1-1 emergency telecommunications system.

Section 5 – USE OF THIS PROCUREMENT BY MULTIPLE DEPARTMENTS

This procurement is being issued as a single Department procurement primarily for use by the State 911 Department. The procurement can also be used by any other public safety department or unit of government within the Commonwealth or quasi-public department or agency or private safety department as the procurement basis for the execution of contracts for the purposes of maintaining, in whole or in part, a PSAP that has been approved by the State 911 Department.

Although eligible entities may utilize this procurement, a separate contract for any such entity shall be executed. The contractor(s) under this RFR shall extend all pricing to such eligible entities, and the contractor(s) under this RFR shall report to the State 911 Department the name of each and every entity with which it has contracted, the dollar value of each and every such contract, and the goods and services thereby provided.

GDIT will comply with the RFR specification.

Section 6 – ANTICIPATED DURATION OF CONTRACT, INCLUDING RENEWAL OPTIONS

The anticipated duration of the contract is five (5) years beginning on the Contract Effective Start Date. The contract will allow for one (1) option to renew for a period of five (5) years. Therefore, the Total Anticipated Contract Duration is five (5) years, plus one (1) option to renew for a period of five (5) years. Therefore, the Total Anticipated Contract Duration, including the renewal options, is ten (10) years from the Contractive Effective Start Date.

Performance and payment time frames which exceed contract duration: At the request of the State 911 Department, the contractor shall be required to complete the performance of any or all projects or project agreements entered into or commenced during the term of the contract whose performance and payment timeframes extend beyond the maximum contract duration end date and/or to work cooperatively with the State 911 Department to undertake all actions necessary to ensure timely project completion.

At the request of the State 911 Department, the contractor shall be required to enter into a maintenance agreement following the expiration of the Contract End Date if necessary to maintain and/or monitor the system or individual system components beyond the maximum contract duration.

GDIT will comply with the RFR specification.

Section 7 – ANTICIPATED EXPENDITURES AND COMPENSATION STRUCTURES

All rates shall become fixed for the initial term of the contract, unless there is a material change to a regulation, guidelines, standard, or order of the State 911 Department or the FCC or other regulatory or governing body that significantly alters the contractor's ability to provide services, as determined solely in the discretion of the State 911 Department. Any renegotiation of rates or pricing resulting from any such material change shall be supported by appropriate and detailed documentation to the satisfaction of the State 911 Department. Further, any renegotiation of rates or pricing at the time of renewal of the contract shall be supported by detailed documentation to the satisfaction of the State 911 Department.

An overall cost/unit estimate is not available. This contract may be funded in part with federal funds.

GDIT will comply with the RFR specification.

Section 8 – PERFORMANCE AND CONTRACT SPECIFICATIONS

General Dynamics Information Technology (GDIT) and our subcontractor teammates welcome the opportunity to support the Commonwealth of Massachusetts in achieving a comprehensive and systemic migration of the legacy Massachusetts emergency services (9-1-1) network to the next generation of 9-1-1 (NG9-1-1) services, capable of supporting multi-modal network communications, location-based distribution, resiliency, and cost savings. **Our solution is fully compliant to the Commonwealth of Massachusetts Request for Response (RFR) State 911 14-002: Next Generation 911 Products and Services.**

GDIT understands the Commonwealth's requirement for a standards-based, National Emergency Number Association (NENA) i3 compliant NG9-1-1 solution that fully accommodates the complex transitional environment across the traditional stakeholder community, including carriers, technology providers, and Public Safety Answering Point (PSAP) operations. Our proposed solution fully considers the primary objectives of achieving high service availability, maximizing security controls, enabling improved maintenance, reducing operational costs through centralized operations, and delivering legacy migration in a low-risk, highly regimented manner to ensure operational integrity.

Proven Processes and Technical Depth. GDIT offers a turn-key solution for the Commonwealth of Massachusetts' NENA-compliant NG9-1-1 initiative that starts with the delivery of a multi-vendor and fully engineered solution, and operationalizes this architecture to deliver the promise of Next Generation emergency communications. We have ensured that our in-place, rigorous program management approach is based on the CommonWay project management methodology. Our program management process is proven and honed in the mission-critical, complex, and highly risk-adverse worlds of the Department of Defense (DoD) and federal agencies to reduce technology and implementation risks, improve Internet Protocol (IP) security and converged services operations, and increase organizational adoption of the new technology. Our technical depth and breadth has been established in the industry with over 20 years of hands-on engineering and project expertise in designing, building, and maintaining complex and highly reliable telecommunications solutions. One example of these capabilities is our support for over 25 years as the single system manager for the U.S. Air Force Air Defense Communications Service (ADCS) contract providing 7-day-a-week, 24-hour-a-day Operations and Maintenance (O&M) support at three Air Defense Sectors (CONUS) and one Air Defense Region (Alaska). This contract supports and modernizes the communications systems and subsystems used in the command and control for Airspace Defense and Homeland Defense by the North American Aerospace Defense Command (NORAD), United States Northern Command (USNORTHCOM), and the Pacific Air Force (PACAF). As the single system manager, we support multiple agencies and end users, and a wide breath of mission-critical technology (telephony, radio, conferencing, analog-to-IP, etc.).

Experienced Systems Integrator. GDIT is a vendor-agnostic systems integrator committed to selecting and delivering the best-fit federated solution that drives cost reduction, ensures technology compliance, and minimizes schedule risk. For Massachusetts, we will be managing a team that consists of industry recognized NG9-1-1 leaders to move the Commonwealth into the new era of emergency services. Our team includes Digital Data Technologies, Inc. (DDTi), Emergency CallWorks (ECW), Synergem, DSS Corporation, Oracle, EMC, Integrated Partners,

Windstream, Winbourne Consulting, Acorn Communications, Fotis Networks, and other diverse and small businesses – many of whom are currently certified by the Commonwealth and some who may be certified after award – as identified in Attachment R2. All of our primary technology teammates have been engaged in collaboration and testing for over a year within the GDIT's **i3 Solutions Interoperability Lab** in Needham, Massachusetts, validating interoperability, performance, and compliance. GDIT recognizes that this is a mission-critical initiative; we will apply our experience and lessons learned as a systems integrator deploying large scale, multi-site projects to this Massachusetts NG9-1-1 project. The result will be a comprehensive set of technology and services delivered by GDIT, providing a high level of confidence to the Commonwealth of Massachusetts.

Best Value. At GDIT, we pride ourselves in quality performance, teamwork, and customer satisfaction. We are committed to delivering exceptional value to our customers. We bring significant experience across a wide array of communications technologies, including legacy E9-1-1 networks, NG9-1-1 systems integration, GIS, TDM-to-IP voice network modernization, security, data centers, and cloud services. Our proposal leverages the significant economies of scale and process efficiencies developed in our partnerships to provide exceptional value. The compelling price point is backed by our extensive experience, proven project management methodologies, and uncompromising dedication to customer satisfaction.

Ready To Go Day One. Our NG9-1-1 multi-vendor i3 Solutions Interoperability Lab has been in place and performed multiple NG9-1-1 functional element tests. Our Needham, Massachusetts facility is ready with sufficient space; Heating, Ventilation, and Air Conditioning (HVAC); and power for the MA NG9-1-1 dedicated lab, and for staging and testing. Our Program Management team and Subject Matter Experts (SMEs) are already in Needham, ready to start.

By choosing GDIT, the Commonwealth of Massachusetts benefits from:

- A world-class systems integrator that has reviewed all specifications, canvassed the industry, identified best-of-breed products element by element, tested, and ensured that the integrated solution is interoperable and meets or exceeds all requirements.
- Decades of experience with large, complex, mission-critical projects that has been applied to this transformation plan with comprehensive risk management and attention to every detail. The submitted Information Technology Infrastructure Library (ITIL) based project plan is thorough and is intended to improve on the Commonwealth's stated goal by achieving completion on April 29, 2016.
- A comprehensive support plan that combines exceptional local help desk and management, centralized operations from redundant Network Operations Centers (NOCs), and local and available support expertise – all managed under a single point of contact for the Commonwealth. Our proactive monitoring and maintenance model ensures maximum network performance and security.
- Our commitment to work collaboratively with the Commonwealth, including adherence to Supplier Diversity Objectives (SDO) and the Americans with Disabilities Act (ADA).

Our solution offers key features and benefits to the Commonwealth of Massachusetts, as shown in Table 1.

Table 1. GDIT Solution Benefits

Feature	Benefit to Commonwealth of Massachusetts
Standards-Based Functional Elements	Interoperable NENA i3 standards-based solution elements to drive down costs, increase efficiency, and minimize service-affecting issues.
System Engineering and Integration Expertise	**Low Technical Risk** – Extensive complex communications systems experience, including a NENA i3 geospatially routed customer deployment. **Proven Engineer, Furnish, Install, and Test (EFI&T) Experience** – Provided well over 1,000 successful system installations/upgrades for Department of Defense (DoD) customers. **Responsiveness** – System Architect and Project Manager proposed with extensive related experience will rapidly resolve design and implementation challenges using a collaborative process.
Disciplined Implementation Approach	**Efficient Performance** – Logical implementation sequence **Schedule Adherence** – Timely and accurate submission and review cycles of deliverables **Management of Changing Carrier Environment** – Optimize connectivity and service transitions **Ready to Begin** – Our proposal includes an installation approach by location. We understand the complexities of this installation and have a comprehensive, well-thought-out approach. **Fully Operational across the Commonwealth on April 29, 2016** – two months before the deadline, well planned and executed with significant cost savings.
Comprehensive Organizational Adoption Plan	**Transition Ownership** – All aspects of the E9-1-1 to NG9-1-1 migration accounted for, including telecommunications service provider interfaces. Collaborative execution beyond technology implementation for long-term success. **Integration with Existing Commonwealth Resources** – Synergy for optimum efficiency. **Multi-Level Training** – Holistic plan that ensures maximum knowledge transfer.
Proactive Security and Network Monitoring	**End-to-End** – Entire call path covered with visibility beyond the end points. **Continuous** – Use of advanced tool sets and trained personnel 24x7x365.
Full Warranty and Maintenance Support	**Complete Coverage** – OEM-included warranty and maintenance is backed by GDIT's 24x7x365 Network and Security Operations Center (NSOC) providing a single point of contact for all support and maintenance issues.
True Fixed Price Proposal	**Compliant Pricing** – As a contractor familiar with performing on large-scale, fixed-price contracts, GDIT's thorough pricing truly meets the Commonwealth's requirements of price inclusion for each and every service and commodity required to be furnished under the RFR.
Financial Stability and Organizational Strength	We bring the financial stability of a Fortune 100 company with over $32 billion in annual revenue and 92,000 employees worldwide to offer low risk to the Commonwealth. Along with employing almost 3,200 people across the Massachusetts, we provide business to over 1,300 Massachusetts-based suppliers, totaling more than $490M in spending dollars over the past two years.
Value-Added Elements of GDIT's Solution	**Broad and Deep Subject Matter Expertise:** As an industry-leading communications Systems Integrator (SI), GDIT has the scope, expertise, resources, and commitment few can offer: • Complex Systems Integration • Geospatial Information Systems • Voice and Video Expertise • OEM-Certified Data and Voice Subject Matter Experts • Data Center and Cloud Technologies • Public Safety • Health Care Information Technology • Military and Law Enforcement • Subcontractor Management Practices • Network Operations Centers (NOCs) • Security Operations Centers (SOCs) • Interoperability Testing **Multi-Point Collaborative Transformation Plan** – Collaboration is built in to every phase of

Feature	Benefit to Commonwealth of Massachusetts
	the project. **Award Winning Training –** GDIT will apply the science of Learning and Performance with our widely recognized Learning Center of Excellence training group. **GDIT NSOC and Windstream Elite NOC Collaboration –** GDIT's 24x7x365 NSOC, staffed by engineers, will partner with Windstream's Elite NOC to provide seamless end-to-end coverage of the entire solution.

The initial task is to finalize the engineered system design. GDIT is committed to delivering a fully documented, standards-based design and establishing critical planning documents for ensuring a smooth migration. A key criterion in selecting the best critical functional elements is the depth of involvement in the standards-setting process.

GDIT's technology team includes the following subcontractor, consultant, and key vendor teammates, all of whom maintain active participation in both GDIT's i3 Solutions Interoperability Lab and NENA Industry Collaboration Event (ICE) testing and collaboration events. Table 2 summarizes the GDIT team and the roles and responsibilities of each team member.

Table 2. Roles and Responsibilities of the GDIT Team

Company	Role and Responsibility	PROVEN PERFORMANCE	
		Proposed System Technology: NG9-1-1 and ESInet Systems	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems
GDIT	• Prime Systems Integrator • Overall program management • Engineering, implementation, and operations lead • Proactive security and performance monitoring • Operations and sustainment	• Providing turn-key Engineer, Furnish, Install, and Test (EFI&T) solution to implement NENA i3-compliant NG9-1-1 solution for Morgan County, Ohio • i3 Solutions Interoperability Lab • MA NG9-1-1 Customer Premises Equipment (CPE) evaluation completed to allow our selection of the best solutions for the requirements provided	• Over 20 years of voice, video, and data implementation, operations, and sustainment. • Sustaining over 500 communications platforms for the DoD and FAA including E9-1-1 (over 70 E9-1-1).
Windstream	• Carrier for IP connectivity to all Commonwealth of Massachusetts site locations • Data Center colocation services • Wide Area Network (WAN) security and performance monitoring	• Providing two proposed data centers and optional third data center. • Competitive Local Exchange Carrier (CLEC).	• Multiple Multi-Protocol Label Switching (MPLS) networks supporting Massachusetts. • 66-site MPLS network, 118-site MPLS network connecting courthouses • 52-site MPLS network including a hub and disaster recovery.

Company	Role and Responsibility	PROVEN PERFORMANCE	
		Proposed System Technology: NG9-1-1 and ESInet Systems	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems
Emergency CallWorks	• I3 Customer Premises Equipment (CPE) product • CPE-related services • CPE implementation and training support • Automatic Call Distribution (ACD) function	• NG9-1-1 call handling and CAD technologies in legacy, networked and hosted models.	• 160 installed PSAPs across the U.S. with over 475 positions. • Multiple successful installations of hosted, networked 9-1-1. • Certified by the Commonwealth of Massachusetts for E9-1-1 call handling.
DDTI	• GIS mapping of Commonwealth-provided data • GIS data normalization • Emergency Call Routing Function (ECRF)	• Support for high-quality Geographical Information System (GIS) data sets – a critical component of the NG9-1-1 solution). • ESInet Location Validation Function (LVF) and Transitional Location Database (LDB).	• Over 1,100 installations in PSAPs nationwide. • Active on various NENA committees and NENA ICE events: ICE3, ICE4, ICE5, and ICE8.
Synergem	• Emergency Services Routing Proxy (ESRP) • Legacy gateways, with related services	• Providing key, essential elements within Emergency Services IP Network (ESInet). NENA i3 ESRP as well as other NG9-1-1 functional elements such as Legacy Selective Router Gateway (LSRG), Legacy Network Gateway (LNG), and Legacy PSAP Gateway (LPG).	• Mission-critical 9-1-1 systems for National Aeronautics and Space Administration (NASA) and the Department of Energy (DOE). • First NENA i3 end-to-end call through ESInet. • Evolution911 graphical user interface for NG9-1-1 capabilities to the dispatcher.
DSS	• Recording/logging and related services	• Flagship communication logger, Equature, is native NG9-1-1 platform. • DSS Equature has been tested at every NENA Industry Collaboration Event (ICE) event to date.	• National installed base of over 1,000 PSAPs. • 270 PSAPs for the Massachusetts State 911 Department.
Aculab	• Provider of gateways and protocol interworking function	• ESInet functional component of LNG.	• Oracle, Synergem, and Aculab ICE integration demonstration.
Oracle	• Border Control Function (BCF) • IP security applications • Quality of Service (QoS) monitoring • Related services	• World leader in SIP session security • ESInet BCF • Voice quality monitoring	• Embedded in system solutions in majority of Tier 1 service providers national networks
Cisco	• IP networking products • IP security products	• Data network routing and switching • Network security devices	• Included in majority of major network designs globally
EMC	• Storage • VDI offering	• Key storage solutions for network management	• Products are currently in use by the Commonwealth

Company	Role and Responsibility	PROVEN PERFORMANCE	
		Proposed System Technology: NG9-1-1 and ESInet Systems	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems

Winbourne	• Public safety Subject Matter Experts (SMEs)
	• Transition and migration planning
	• Carrier liaison
		• Subject matter expertise:
		  • NG9-1-1
		  • Public safety migration
		• Training
			• Multiple E9-1-1 SMEs support State, County, and Police Department implementations.

Integration Partners	• Field service • System Installation	• Providing network operation and implementation support • Long-term life cycle sustainment	• Commonwealth of Massachusetts systems integrator

Migration. The Commonwealth of Massachusetts' transition is not just about technology; it must include full consideration of timing impacts on costs, organization adoption, and overall risk mitigation. This is a fundamental shift from a vertical, proprietary solution to one that is standards-based and inherently interoperable. A trusted partner who is vendor agnostic and large enough to manage the transition through a time-sensitive period becomes a key factor for success. Interoperability, risk management, operational enablement, life cycle support, customer service, and training will be critical to a successful transformation. We illustrate our rigorous, multi-tiered engineering approach, based on Information Technology Infrastructure Library (ITIL) quality practices, in Figure 1.

Figure 1. Multi-Tiered Engineering Approach

Using our multi-tiered engineering approach, we are currently bringing all of these capabilities to bear on the NENA i3-compliant NG9-1-1 production deployment for the State of Ohio (by county) with a fully functioning Emergency Services IP Network (ESInet) with spatial routing, based on geographic coordinates. Our ongoing Ohio project is a complete NG9-1-1 construct with adherence to NENA standards, fortified by intelligent engineering to bridge gaps in the standards, and tempered by well-conceived implementation strategies to improve cost-effectiveness without diminishing overall compliance. The Ohio project is has gone through multiple readiness tests and is expected to go live as soon as carrier connectivity is provided by the Commonwealth.

Shortened Schedule: Throughout the phased approach, GDIT will provide technical and project management that ensures communications across all stakeholders and management of subcontractors, and identifies formalized documentation and planning. We will work to our negotiated schedule, and gain approvals as we progress from each phase, providing the appropriate validation testing and security audits. Our detailed understanding of the activities associated with the phased implementation; comprehensive turn-key approach to successful, low-risk program execution; and deep bench strength *allow us to deliver NG9-1-1 to the Commonwealth of Massachusetts two months ahead of the deadline.* **All implementation phases will be complete and the Commonwealth resources fully trained by April 29, 2016.** From that point forward, you can continue to rely on team GDIT for a highly available, reliable, and secure solution that will deliver the full benefits of NG9-1-1 to the citizens of Massachusetts.

Summary of the GDIT Approach

GDIT, as the prime contractor, will be accountable for the solution and services over the entire period of performance. We have extensive experience in delivering mission-critical communication solutions, including extensive E9-1-1 system deployments and seamlessly evolving complex legacy networks to converged IP services. We have already established our NG9-1-1 NENA i3 Solutions Interoperability Lab to test multiple vendors' functional elements separately, with an objective of optimizing the end-to-end solution. We look forward to a partnership with the Commonwealth of Massachusetts to provide a low-risk and high-availability project migration. GDIT applies over 20 years of mission-critical voice operations and sustainment expertise, providing Massachusetts with a 24x7x365 single point of contact for support and maintenance. We emphasize our voice and unified communications expertise because real-time services – particularly TDM-to-IP voice migration in a centralized hosted environment – requires a unique set of skills and demands experience that few contractors can offer.

8.1. PROJECT OVERVIEW

The State 911 Department is seeking a Next Generation 911 emergency telecommunications system that shall possess the highest degree of resiliency, reliability, redundancy, and service availability. The system shall support the delivery of 911 voice calls to all PSAPs located throughout the Commonwealth. The system shall be compliant with the NENA i3 standard.

Although the initial deployment shall support voice calls and text messages, it is the objective of the State 911 Department to procure a system that shall comply with evolving national standards, and that shall offer the functionality to support Next Generation 911 capabilities, including without limitation, the delivery, receipt, and Therefore, bidders shall respond with proposals for a system that either currently supports, or will support in the future, such Next Generation 911 payloads as are generally accepted within the emergency services community.

Non-performance or delay in performance by the service provider may result in disruption in delivery of services, and, therefore, time is of the essence in performance dates, deadlines, and delivery dates.

The system shall be fully operational throughout the Commonwealth no later than June 30, 2016. This deadline shall be strictly adhered to and shall be strictly enforced.

In order to meet the hard deadline of June 30, 2016, extensive upfront solution, network and failover testing, in addition to upfront process development, is required to ensure that the deployment phase of the project runs seamlessly with all the issues being brought to light during the design and testing phases.

The migration to the Next Generation 911 system shall be on a rolling basis. The project schedule and any changes thereto, including the sequencing of the installation at the PSAPs, shall be subject to the approval of the State 911 Department. Since the migration to the new service will be conducted in stages, the response shall set forth the bidder's plans regarding the support of a phased migration, rolling staged cutover, and parallel operation and provision of gateways to legacy systems and networks. Limited secondary PSAPs shall be deployed simultaneously with the primary PSAP or regional PSAP that is served by the limited secondary PSAP.

The contractor shall be required to directly interface with other Commonwealth agencies, including without limitation, MassGIS for GIS-related activities.

Bidders are encouraged to use their knowledge and products to respond with the system that provides best value for the Commonwealth.

Responses shall address, at a minimum, the following high-level components:

- *Network design, management, and operation;*
- *Applications and appliances, including connecting devices, routers, firewalls, and other components required to transmit payloads from the border control function through the i3 functional elements to the appropriate PSAP;*
- *Applications and appliances in data centers;*
- *Devices capable of recording payload information as delivered to the ESInet in a manner consistent with diagnostic timing and functional element failure;*
- *Integration plans for applications and appliances, including design components and certification of i3 compliance;*
- *The services of a help desk, NOC, and system failure resolution;*
- *Installation, testing, and acceptance processes;*
- *Approach to a phased cutover and transition/migration of installed base*
- *in data centers, laboratories, training centers, and PSAPs;*
- *High function/performance capabilities in data centers;*
- *Ongoing operation of the system;*
- *Project management for the installation, testing, and certification of the system; and*
- *Warranty and maintenance.*

Bidders shall supply a response that fully describes in detail their overall effort.

The system shall be expandable. Such expansion shall be on an incremental basis, not a wholesale replacement of major platform(s). The contractor shall certify that subsequent system expansions or upgrades will be backward compatible with components proposed herein. Bidders shall describe the scalability and expandability, indicating the related costs of the system in terms of its various components.

Bidders shall describe in detail all system needs and requirements to support and implement the system to be delivered by the contractor.

GDIT will comply with the RFR specification.

GDIT's proposed turn-key network and applications solution for the Commonwealth of Massachusetts NG9-1-1 Emergency Communications System (MA NG9-1-1) is aligned with the Commonwealth's MassNet vision, is NENA compliant, and offers the following features:

- A highly-resilient architecture designed for 99.999% availability, including redundant Wide Area Network (WAN) paths and PSAP access circuits; load balancing between data centers, and Multi-Protocol Label Switching (MPLS) Quality of Service (QoS) technology to support voice service quality and prioritization.
- A robust, multi-level, defense-in-depth security architecture provided by GDIT, one of the leading cyber security integrators for the U.S. federal government.
- A robust Network and Security Operations Center (NSOC) and Help Desk using ITIL best practices to ensure operational efficiency and customer service.
- Massachusetts-based personal providing architecture, engineering, program, and project management by GDIT, one of the nation's largest EFI&T contractors. Experience successfully implementing well over 2,000 projects, many of which are national or global in scope.
- A low risk deployment approach, including a dedicated Transition/Migration Liaison, that targets delivery by April 29, 2016 – a full two months ahead of the required delivery date.
- Scalable and expandable for current and future Commonwealth public safety needs, including providing access to GDIT's NENA i3 Solutions Interoperability Lab in Needham, MA to allow evolution and future modifications as NENA standards evolve, to include backward compatibility.

The GDIT team, introduced in Table 2 earlier in our proposal, consists of industry leaders who play an instrumental role in establishing NENA standards and participate in Industry Collaboration Events (ICE) – which are recurring forums to substantiate interoperability and compliance with NENA standards. The planning, design, testing, and transition efforts for GDIT's NENA i3-compliant turn-key solution will be performed in close partnership with the Commonwealth, enabling the Massachusetts Executive Office of Public Safety and Security (EOPSS) to help shape and influence future evolving NENA standards based on real-world needs. GDIT is currently teamed with some of our proposed strategic subcontractors/vendors (DDTi, Oracle, and DSS) in providing a NENA i3-compliant NG9-1-1 production deployment for the State of Ohio.

Additionally, we have teamed with Competitive Local Exchange Carrier (CLEC) Windstream to provide data center services as well the physically diverse carrier topology. Windstream has a proven track record within the Commonwealth of Massachusetts. Through the PAETEC acquisition, Windstream has provided network related services to the Commonwealth for over eight years. As an ITT09 contract holder, Windstream is also a participant on the ITT46 contract. As detailed in Section 9 (Bidder Qualifications) of this proposal, Windstream has managed two successful large-scale projects for the Commonwealth Information Technology Division (ITD) and Massachusetts Trial Courts.

Figure 2 provides a view of the NG9-1-1 reference architecture of the GDIT solution, while the following paragraphs summarize our technical approach. The detailed technical solution descriptions are contained in Section 8.3 through Section 8.24.

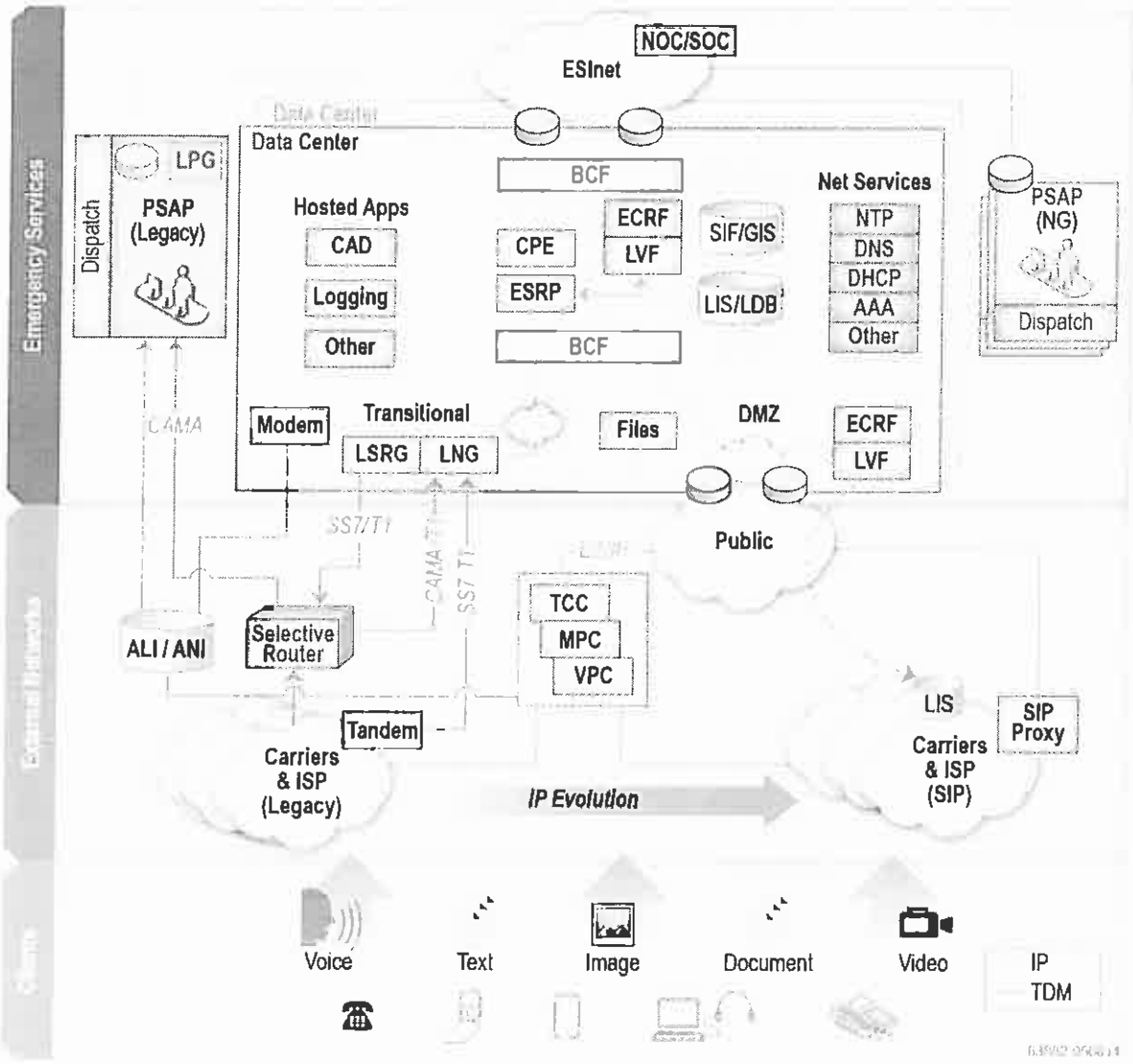


Figure 2. GDIT NG9-1-1 Reference Architecture

GDIT fully understands that NG9-1-1 is more than just a technology solution. First and foremost, NG9-1-1 is a public safety medium that enables lifesaving services to be delivered throughout the Commonwealth. The GDIT team comprises companies that have intimate knowledge of public safety requirements and are staffed with personnel who have provided many years of service within the public safety community.

The GDIT team also understands that NG9-1-1 is about firsts: new technologies, integrated solutions, and adaptive communications. The public safety industry is under ever-increasing pressure to transition to NG9-1-1 to enhance capabilities and services that protects and serves an ever-evolving technological society.

Product and Technology Roadmap

In regard to the "Product and Technology Roadmap," our product teammates for the Massachusetts NG9-1-1 project are actively involved with various NENA and ICE committees and activities developing standards and test events. For example, our key subcontractors Synergem, DSS, and DDTi, and selected vendors Oracle and Aculab, led and actively participated in the recent ICE 8 planning committee in November 2013. Our team is acutely aware of the evolutionary roadmap for further development and refinement of NENA i3 standards along with wider-scale NG9-1-1 implementation efforts and initiatives.

The NENA i3 standards are being updated to address clarifications and enhancements in a number of technical areas, but which will not require any fundamental changes in the architecture. The NENA standards are revised in an iterative process that has recently experienced up to four-year intervals between major changes, with ongoing updates as new technology is introduced or regulations change.

Table 3 is a sample of some of the product and technology roadmaps for current and future features and functionality that are planned to be added.

Table 3. Product and Technology Roadmap Example

Product OEM	Description	Targeted Completion Date
DDTi	GIS Data Extract, Translate and Load (ETL) tool to facilitate the import and redistribution of GIS data	Q3 2014
	NENA compliance review and product modifications to ensure all products meet the latest published standards	Ongoing
	Management tool enhancement for ECRF/LVF	Q4 2014
	Validation/Geocoding Services	Q1 2015
	GIS data maintenance editor enhancement	Q2 2015
	AVL integration into ESRI-based call taker map display including geofencing and incident mapping capabilities enhancement	Q3 2015
	Scalability and robustness validation of NG9-1-1 services (ECRF/LVF, LDB, DataLoad, and map display).	Ongoing
DSS	SysLog – Audit Trail records enhancement	Q2 2015
	SNMPv3	Q1 2015
Aculab	Configuration interface upgrade for QoS marking of RTP	Q1 2014
	Windows configuration for QoS marking of SIP signalling traffic (Server 2008 platform) documented in User Guide	Q1 2014
	Mapping of User-to-User Indications (UUS1) to SIP (User-to-User Header), from ETS 300 and QSIG	Q1 2014
	Mapping of calling and connected party names, from QSIG to SIP (Remote-part-ID header)	Q1 2014
	Configuration Interface upgrade for QoS marking of RTP	Q1 2018
	Interworking of the implicit UUS1 service between SIP and EuroISDN, using the 131-octet standard	Q2 2014
	TDD/TTY-to-RTT transcoding/interworking	Q1 2015
	Routing of calls on a per SIP route basis	Q1 2015
	IPv6 support	Q2 2015

Product OEM	Description	Targeted Completion Date
Oracle	Enhance Rich Communication Services (RCS) capabilities and expand Lawful Intercept (LI) capabilities	Q3 2013
	RCS enhancements for Linux SMP operating system	Q3 2013
	Diameter Policy and Accounting enhancement	Q4 2013
	Diameter Policy and Accounting and Optimized Media Routing (OMR) enhancements	Q3 2014
ECW	NENA compliance review and product modifications to ensure all products meet the latest published standards	Ongoing
	CAD enhancements	Q4 2014
	Increased Scalability and Availability parameters	Q4 2014
Synergem	NENA compliance review and product modifications to ensure all products meet the latest published standards	Ongoing
	Portfolio expansion to include enhanced ACD platform	Ongoing

In addition to OEM product roadmaps, GDIT – under the guidance of the Chief Technology Officer (CTO) office – conducts recurring technology summits on topics such Unified Communications, Cyber Security, Mobility, Software Development, Big Data, and Logistics. None of these summits are closed door, and we regularly invite customer and partner participation. We will leverage our i3 Solutions Interoperability Lab to test and demonstrate new product roadmap offerings, and we will also conduct **user conferences** for the sharing of information and open communications.

User conferences hosted for other GDIT programs have included: technology sessions sponsored by OEMs, training sessions geared toward enterprise transition or refreshers, and panel discussions. As part of our organizational approach, we have formed an Executive Advisory Committee with participants from each of the partners. This committee is involved in consulting and collaborating with the program team on important technical and business topics.

The following is a high-level technical overview of the overall solution with pointers leading to more detailed technical information elsewhere in our proposal.

Network Design, Management, and Operation

GDIT's proposed network design (Figure 3) is redundant, physically diverse, scalable, and flexible to meet the Commonwealth's current and future public safety requirements. GDIT will work in close partnership with the Commonwealth in developing the final approved detailed network design. The physical architecture combined with the routing architecture provides the Commonwealth with the highest availability, reliability, and highest-quality NG9-1-1 network available today. The routing network design architecture is based on Cisco products utilizing standards-based protocols.

For additional technical detail, please see Section 8.3, ESInet.

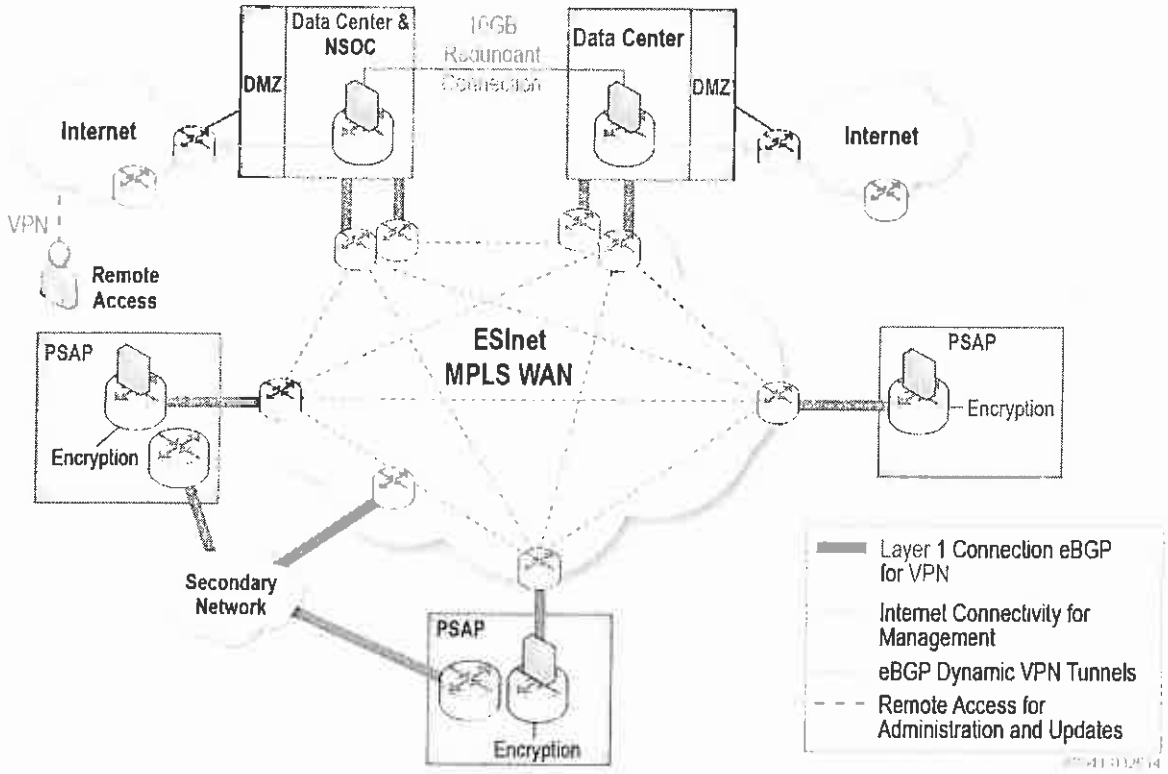


Figure 3. GDIT's Proposed Network Design. Redundant, physically diverse, scalable, and flexible to meet the Commonwealth's current and future Public Safety requirements

The Wide Area Network (WAN) and data center architecture consists of two geographically dispersed data centers within the Commonwealth: one located in Andover, MA and one located in Springfield, MA. The data centers are connected via two carrier-diverse and physically diverse 10 GB links that are being provided by our partner Windstream (see Figure 4).

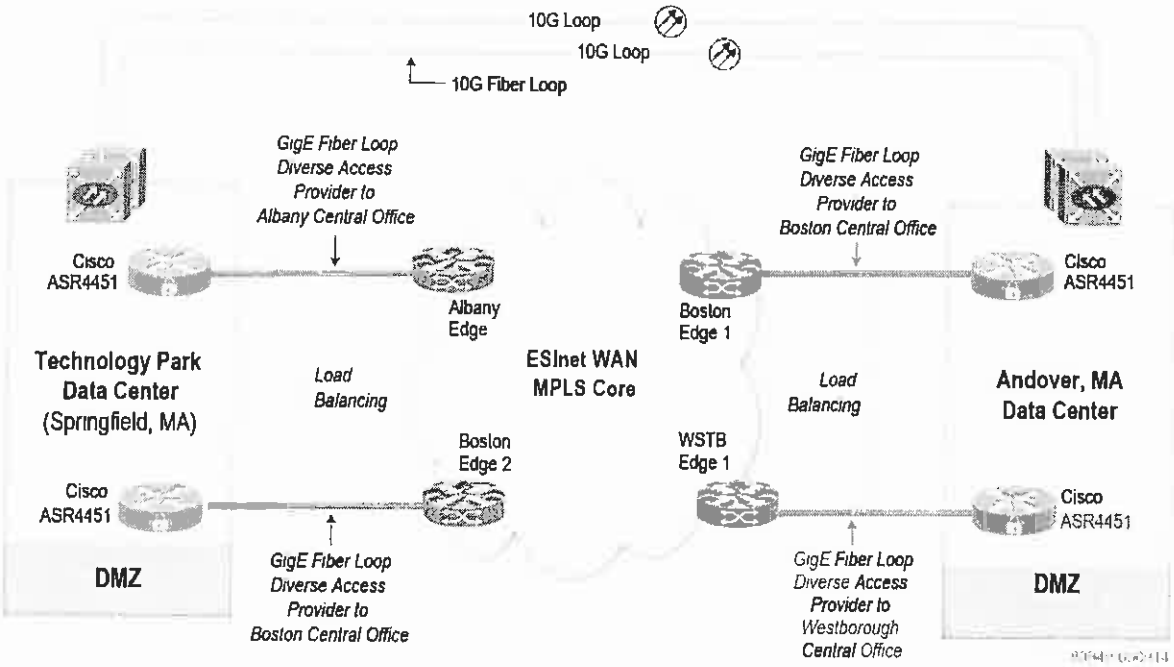


Figure 4. Data Center Network Topology. Each data center is provided with redundant access to diverse WAN central offices. This assures that no single point of failure can disrupt service delivery.

The ESInet architecture provides comprehensive high availability of all systems and applications within each data center with full redundancy between data centers, ensuring "five nines" (99.999%) of availability. GDIT is partnered with Competitive Local Exchange Carrier (CLEC) Windstream to provide data center services as well the physically diverse carrier topology. Windstream utilizes a variety of network assets to provide a redundant, geographically diverse network within the Commonwealth for the Massachusetts Trial Courts, the Executive Office of Labor and Workforce Development, and the Office of Information Technology Division. GDIT also has a close working relationship with Windstream on other NG9-1-1 projects, which provides the Commonwealth with a proven solution.

Dual and diverse circuits from each carrier will terminate at each data center and enter the ESInet as an IP Session Initiation Protocol (SIP) call through the Legacy Network Gateway (LNG). The "traditional carrier voice traffic" termination to the LNG is the point of demarcation where traffic enters into the ESInet.

GDIT's solution provides the Commonwealth with two ESInet access points, one in each data center. The ESInet terminates within each of the data centers and is connected via physically diverse and redundant GAB point-to-point private circuits to the Windstream edge routers at their Central Offices. The ESInet network and application design is highly redundant and designed for failover between each data center. Each data center and ESInet is designed to support 100% of all Commonwealth NG9-1-1 traffic in the event of a catastrophic failure of a data center, WAN, PSAP, or ESInet. For more information on the detailed ESInet design, please see Section 8.7, Next Generation 9-1-1 Architecture.

The physically diverse and carrier-diverse WAN network topology, combined with the redundant ESInet architecture, will provide 99.999% availability as specified in the RFR. The Andover data

center is a former Commonwealth of Massachusetts 9-1-1 data center that Windstream has acquired and upgraded, and the Springfield data center (located at 1 Federal Street) is an Axia/Massachusetts Broadband Initiative (MBI) hub. GDIT has received a commitment letter for data center space at the Springfield, MA location. Windstream has an existing Network-to-Network Interface (NNI) at this location and is already working on a wide variety of projects in conjunction with MBI.

GDIT has evaluated multiple options for the optional third data center and stands ready to support the Commonwealth when that effort is initiated. We propose the Windstream Hosted Solutions McLean Data Center in McLean, VA. GDIT recommends the Commonwealth execute the third data center option when the selective routers are decommissioned and the carrier voice traffic is IP-based for cost-effective out-of-state IP-based call routing. GDIT has included the third data center option costs within the Pricing Response of the proposal.

The PSAP network design provides fault-tolerant connectivity from the PSAPs into the primary ESInet WAN backbone, and also provides fault tolerance and redundancy via diverse dual-path circuits that utilizes the MBI as a secondary path for PSAPs (see Figure 5).

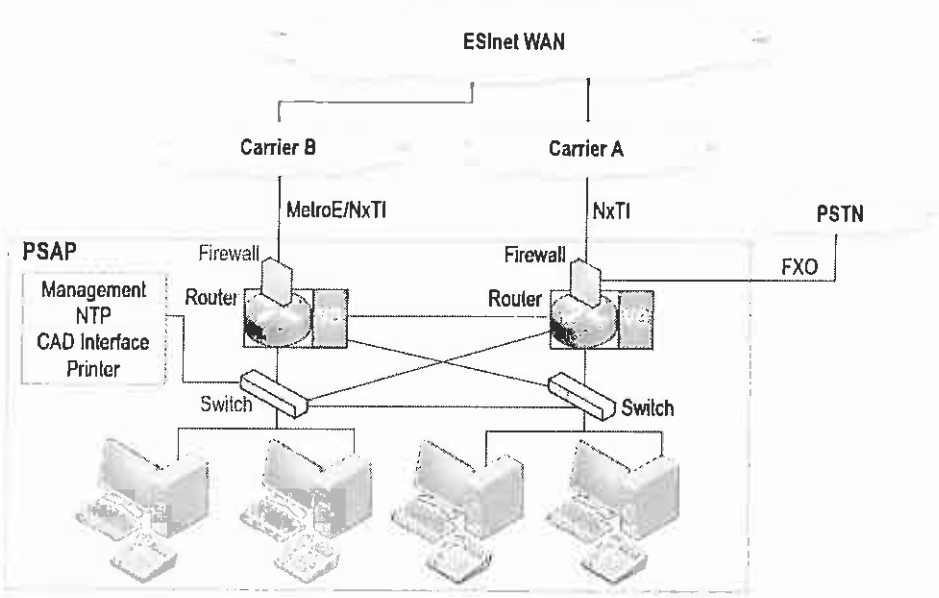


Figure 5. Medium-Sized PSAP. Dual redundant PSAP access circuits ensure fault tolerance.

PSAPs containing 20 positions or more will have minimum redundant MOB carrier Ethernet links to the redundant WAN architecture as well as a MOB fixed wireless tertiary path where line-of-sight is available (see Figure 6) Other locations without line of sight fixed wireless are supported via Satellite. Details on PSAP bandwidth information can be found in Attachment F.

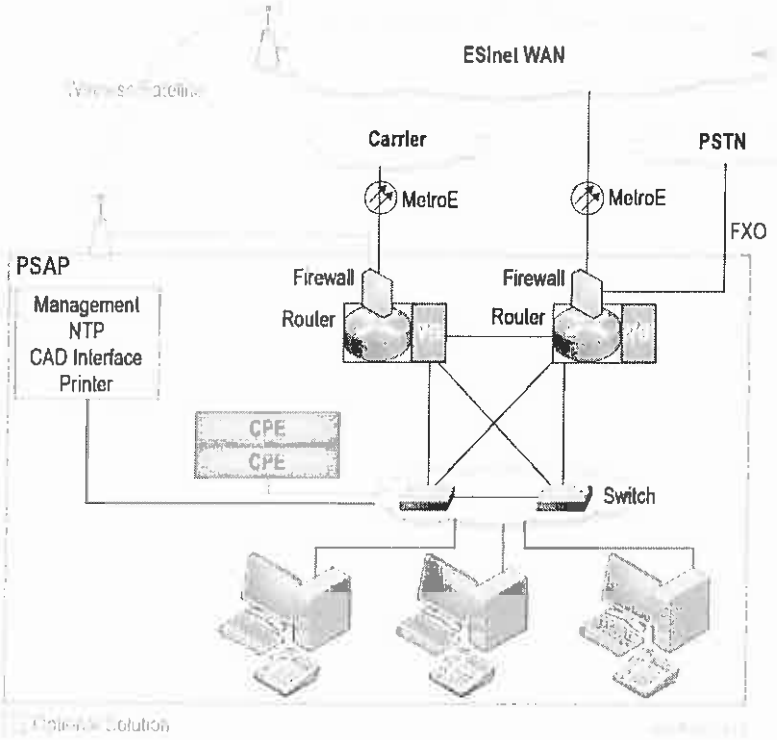


Figure 6. Large PSAP. PSAPs with 20+ operator positions will have a minimum of MOB dual redundant access circuits.

NG9-1-1 IP multimedia traffic will flow to/from each PSAP to the data centers containing the ESInet(s) utilizing intelligent IP routing. The network design includes redundant, dual Ethernet switches and, as required, dual routers at PSAPs identified by the State 911 Department. To ensure the voice quality of the caller and call taker, the PSAP and data center routers and switches will apply Quality of Service (QoS) markings throughout the ESInet environment. Windstream's MPLS Real-Time-Services (RTS) are used to connect those routers across the WAN and ensure end-to-end QoS.

The QoS design allows NG9-1-1 voice quality to remain at the highest level, especially during critical events that tend to invoke high call volumes, massive data transfers, and information search queries. The WAN edge switches will establish the QoS policies and apply markings for:

- Priority 1: NG9-1-1 voice
- Priority 2: NG9-1-1 data
- Priority 3: NG9-1-1 administrative and Network Management System (NMS) packets
- Priority 4: Other non-NG9-1-1 traffic

The WAN edge router will inspect these QoS attributes to ensure traffic policies are intact and reapply QoS attributes as necessary. The GDIT team will work in close partnership with the Commonwealth to develop an approved final network design that includes all necessary QoS settings. The GDIT network design solution is highly resilient and flexible to meet the current and future Commonwealth public safety needs including security.

Network Security

As shown in Figure 7, security is pervasive throughout the network design. The core cyber security design is based on the defense-in-depth methodology, which incorporates cyber security at the network edges as well as in the fabric of each network device. The security layering allows each mission-critical application and function to remain independent and isolated from each other.

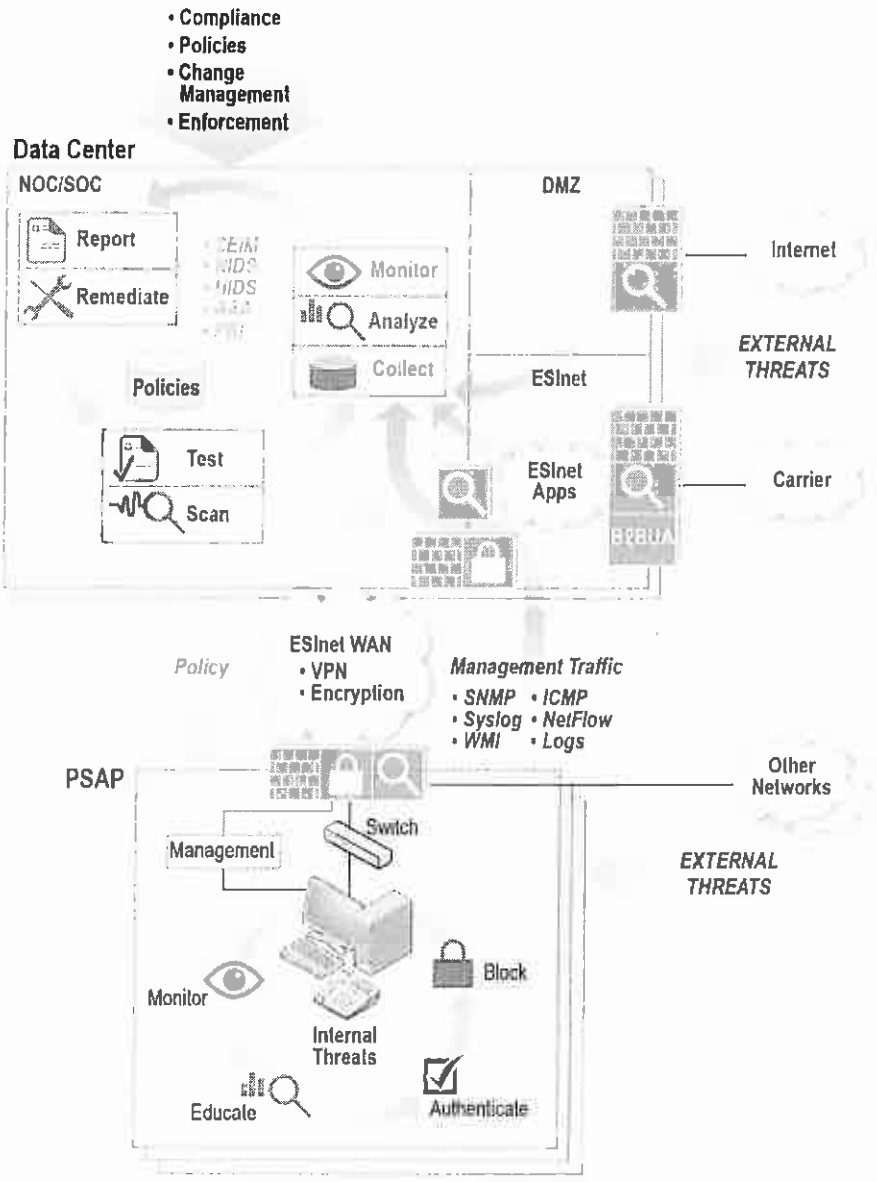


Figure 7. High-Level Overview of the Security Configuration

The perimeter (untrusted network or physical location) is hardened with a combination of firewall layering and intrusion protection. The network and routing design offers multiple levels of defense-in-depth security features, which are layered to form a hardened perimeter and to

monitor internal traffic flows – ensuring a continuous threat detection and prevention environment. Security is a critical element in network design to protect the overall topology including the NG9-1-1 ESInet.

Additional technical detail can be found in Section 8.4, Network Security, Network Security.

Applications, Appliances, and Design Components

The ESInet design components identified in Figure 2 are provided by GDIT teammates who provide state-of-the-art NG9-1-1 compliant solutions:

- **ESInet Border Control Function (BCF)** provided by Oracle.
- **Emergency Services Routing Proxy (ESRP)** and the Location and Network Interface Function (LIF/NIF) components of the **Legacy Network Gateway (LNG)** will be provided by Synergem. Synergem operates exclusively in the public safety emergency communications sector governed by NENA and has developed one of the nation's only solutions that complies with NENA i3 standards.
- **Protocol Interworking Function (PIF) component of the Legacy Gateways** provided by Aculab, which is the functional component of the LNG that interworks legacy Public Switched Telephone Network (PSTN) signaling (such as Integrated Services Digital Network User Part (ISUP) or Centralized Automatic Message Accounting (CAMA)) with Session Initiation Protocol (SIP) signaling.
- **Geographical Information System (GIS)** solution including the ECRF/LVF and Location Database (LDB) will provided by DDTi is the only company recognized by NENA with a certificate of appreciation for outstanding contribution made to the ECRF/LVF i3 standards. GDIT's solution includes comprehensive interface with MassGIS to present accurate location, mapping, and imaging to call taker positions.
- **IP Automatic Call Distribution (ACD) Customer Premises Equipment (CPE)** solution, including the call taker interface, is provided by Emergency CallWorks (ECW). ECW's solution is a web-based, centralized approach to CPE that will provide the Commonwealth significant capability and flexibility while reducing ongoing operational costs.
- The **Digital Logging Recorder (DLR)** solution is provided by DSS Corporation. DSS's experience includes a nationally installed base of over 1,000 PSAPs including 270 PSAPs within the Massachusetts State 911 Department.

Additional technical detail can be found in Section 8.7, Next Generation 9-1-1 Architecture

Network and Security Operations Center (NSOC) and Help Desk

NSOC. GDIT's solution incorporates comprehensive state-of-the-art network management, security management, and help desk capabilities as a fundamental enabler of quality, reliability, and service delivery. GDIT's NSOC is an integrated solution with a maintenance and repair approach utilizing our 24x7x365 NSOC located in Needham, MA, with a backup 24x7x365 Network Operations Center (NOC) located in Fairview Heights, IL. The GDIT team utilizes an integrated Network Management System (NMS) and Security Information and Event

Management (SIEM) solution that consolidate a suite of monitoring tools and methods to provide proactive notification of server or service-affecting events including proactive security monitoring. These methods include automated messaging sent from management and monitoring systems that notify personnel directly without any human intervention, should a service be down or impaired. Sensor-based environmental and power system monitoring is performed at each of the data centers with automatic notification to the NSOC of any conditions that exceed defined thresholds. Commonwealth staff will also be trained on the NSOC systems, procedures, and NMS to facilitate possible future transition of the operations by Commonwealth personnel. The State 911 Department will be given access to the NMS tools and reports via a secure, web-based interface.

Additional technical detail can be found in Section 8.20.7.3, Network Security and Operations Center.

Help Desk. Unlike most companies that provide non-technical staff who simply answer calls, GDIT's 24x7x365 Help Desk provides a complete solution as a center of excellence that is staffed with highly qualified, technically certified personnel, and operates as an extension of the NSOC. GDIT's Help Desk will be located in Needham, Massachusetts with a dedicated toll-free service number to provide Single Point of Contact (SPoC) support for the Commonwealth's NG9-1-1 solution. GDIT's Help Desk utilizes BMC Remedy to open, track, remediate, confirm and close tickets using processes based on Information Technology Infrastructure Library (ITIL) best practices. The solution meets all escalation and response times specified in the RFR. The State 911 Department will have remote access to view and track tickets within the BMC Remedy system as well as view reports. The GDIT NSOC and Help Desk have tightly integrated installation, testing, and acceptance processes as part of a seamless approach to transition and overall program management.

Additional technical detail can be found in Section 8.20.7.1, Help Desk.

Installation, Testing, and Acceptance Processes

GDIT's deployment strategy aligns with the long-range goals of the Commonwealth and its MassNet vision. GDIT's proposed network architecture conforms to the roadmap of MassNet, which provides the Commonwealth a framework supporting a sequential and phased transition.

GDIT will use a phased approach for completing the transition to the NG9-1-1 architecture and aligns to Milestone 4 PSAP transitions. GDIT will work in close partnership with the Commonwealth to gain official approval to move into the Build/Test phase. Prior to any cutover or transition of the Commonwealth's installed base, extensive training and testing will be performed along with a detailed Cutover Plan to be approved by the Commonwealth. Cutover Plan approval will lead to formal Authorization to Proceed (ATP) for each transition cutover. Figure 8 provides an overview of our phased and rolling-base schedule and migration approach.

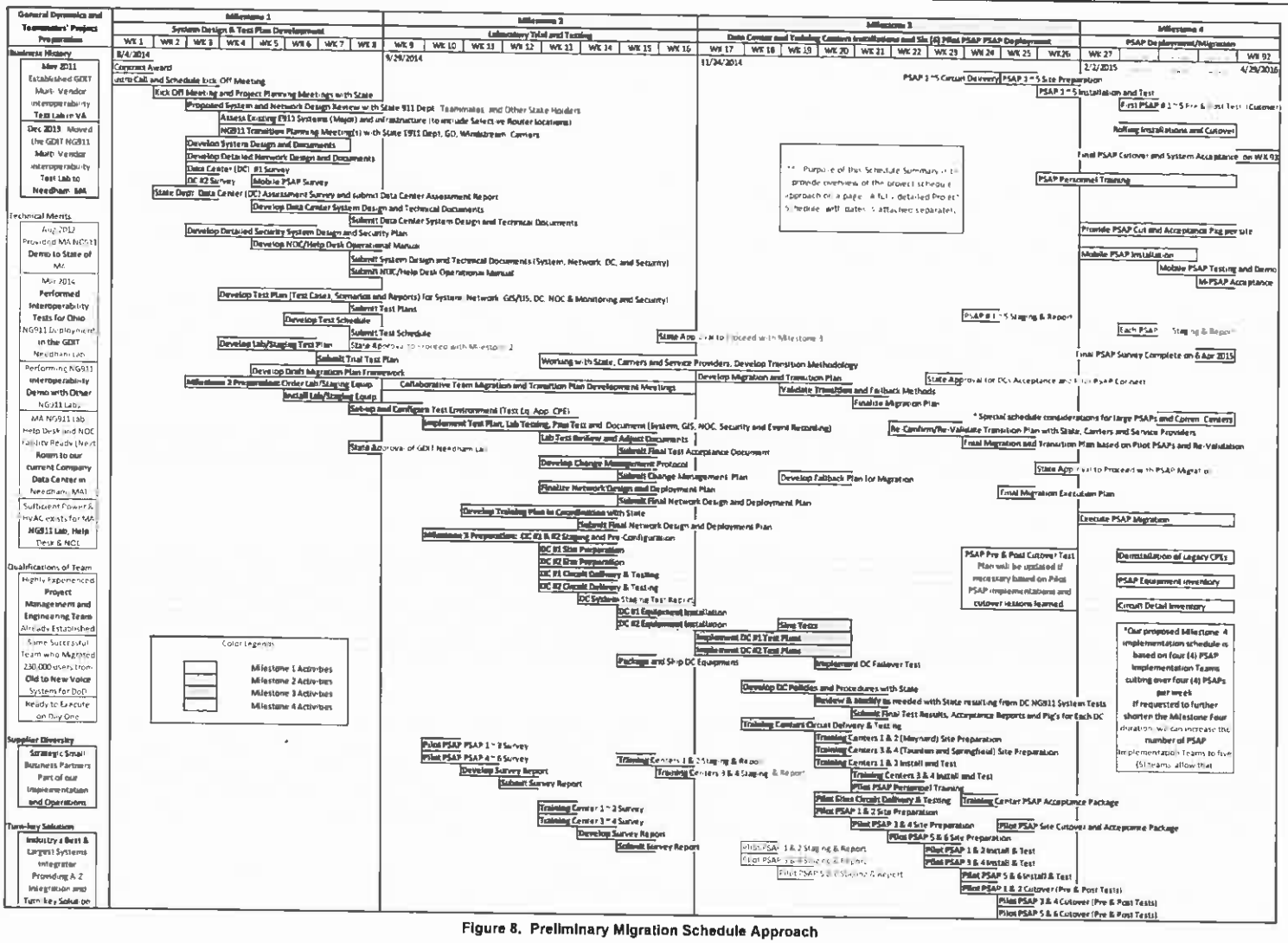


Figure 8. Preliminary Migration Schedule Approach

As part of the Planning process, GDIT has created a detailed plan that will include an actionable Integrated Master Schedule (IMS) detailing timelines, critical paths, deliverables, and resources. The detailed plan will also include a risk assessment matrix to ensure that the Commonwealth has visibility into GDIT's risk management and mitigation before moving into the Design phase. GDIT is submitting an initial, realistic IMS for Commonwealth review along with this proposal submission. This initial IMS will be further enhanced in close partnership with the Commonwealth after award.

The Design phase will include all necessary documentation for the Commonwealth to review and approve the overall design. This design package will include, as a minimum:

- Detailed and final designs for:
  - ESInet (NG9-1-1 Routing and Applications)
  - Data Centers
  - Network and Security Management
  - Applications, Appliances, and Devices, including (but not limited to)
    - Routers
    - Firewalls
    - Other components required to transmit various payloads from the BCF through the i3 functional elements to the PSAPs
- Detailed transition plan
- Installation and acceptance testing procedures
- Operations and sustainment design, including:
  - Network and Security Operations Center (NSOC)
  - Help Desk
- Spare parts strategy and warranty and maintenance plans

Based on our analysis of the program schedule, GDIT has determined that the following system activities, builds, and testing can occur in parallel with ongoing operations:

- GDIT NG9-1-1 Laboratory staging and testing including simulated PSAP position
- Data center redundant failover configurations
- Highly-redundant ESInet builds in two geographically dispersed data centers
- PSAP IP network equipment instantiation (aligned with Milestone 4)
- PSAP router and switching configurations (aligned with Milestone 4)
- PSAP IP circuit termination, testing, and acceptance (aligned with Milestone 4)

By conducting the above activities in parallel, GDIT is able to accelerate the schedule for delivery of the initial PSAP capability to April 29, 2016, two months ahead of the Commonwealth's requirements.

Along with the deployment, GDIT will provide for Commonwealth approval a training environment. This training environment will be one of the initial installations during the Build/Test phase and will be used to support functionality acceptance testing and to provide Just-In-Time (JIT) training prior to the production rollout. This will ensure that PSAP position

migration will occur on the heels of recently conducted i3 Customer Premises Equipment (CPE) training.

This approach to parallel system configurations and testing will ensure all environments are ready for transition into production while accelerating the overall schedule by two months, yet still ensuring no impact to ongoing operations occurs.

The Build/Test phase will also include the implementation and acceptance testing of the GDIT NSOC and Help Desk as well as performance reporting. GDIT will work in partnership with the Commonwealth to gain approval to move from the Build/Test phase into the Operate phase, where PSAP migration occurs.

Additional details on the installation, testing, acceptance and transition is contained within Section 8.13, Migration, Deployment, and Installation.

Project Management

Successful delivery of the MA NG9-1-1 project requires a disciplined project management approach combined with deep technical and integration skills not traditionally found in the legacy 9-1-1 space. This program requires multiple disciplines and skill sets to transition from, and connect to, disparate platforms.

As one of the largest systems integrators in the United States, GDIT's capabilities and expertise includes complex program management, security management, network management, transition planning, and other unique skill sets that are crucial on a project of this scale and scope. As a premier systems integrator, GDIT has assembled a team of customer-focused partners with core competencies that, when packaged as a total solution, comprise the most effective and lowest risk migration path for the Commonwealth.

GDIT's Massachusetts-based team and NENA i3 Solutions Interoperability Lab provide easy access for government oversight during system development, as well as providing a development platform for future evolution of system capability.

GDIT's program and project management is based on the "CommonWay" project management methodology with each life cycle phase tightly integrated with the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK). Figure 9 provides a high-level overview of how each life cycle phase aligns with CommonWay and PMI's PMBOK.

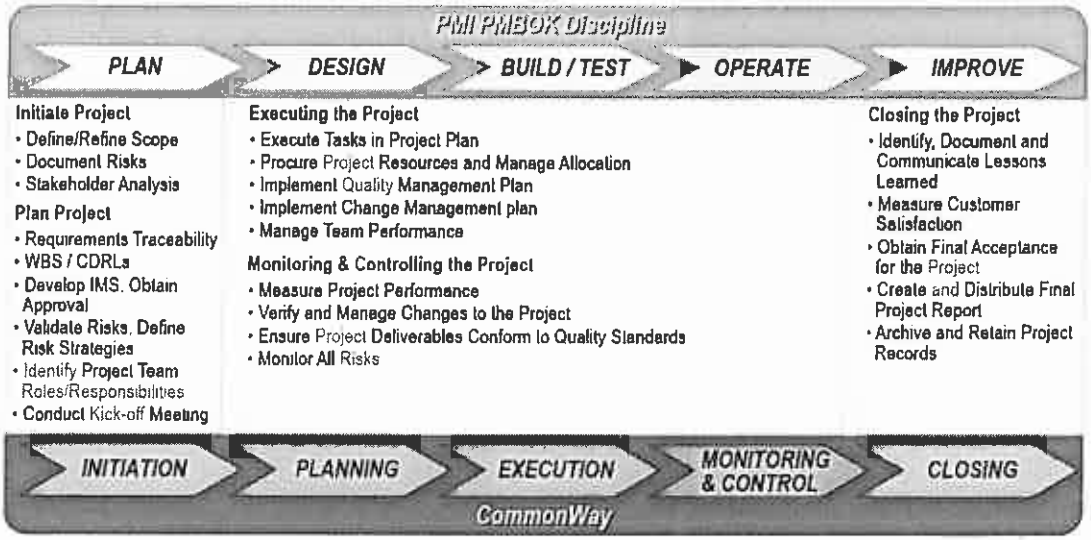


Figure 9. GDIT's Approach for System Life Cycle Management. Our approach adopts the Massachusetts CommonWay project management methodology, which is closely aligned with the PMBOK.

GDIT brings a full suite of project management tools and processes that are the foundation for effective project management and efficient technical activities. These processes and tools provide:

- A repeatable set of processes for use by Project Managers and Technical Leads to ensure operational efficiency and overall quality performance
- Best practices and lessons learned from previous programs. Our standardized processes incorporate those best practices and lessons learned to enhance efficiency.
- A common foundation and knowledge repository for GDIT and subcontractor use, creating a common baseline for knowledge sharing, employee, and subcontractor training.
- Tailoring of standards and tools to the requirements of Massachusetts NG9-1-1 project so that all technical activities are relevant, efficient, and optimized.
- A framework for maintaining and continuously improving the standards and project management tools to ensure Quality Assurance (QA) in all areas.
- Integration between tools (management, program, and technical) and standards for monitoring and reporting to guarantee effective management of this complex, multidisciplinary projects.

Integrated Master Schedule (IMS). GDIT has developed a detailed IMS for the Massachusetts NG9-1-1 project that not only meets all project milestones, as shown in the attached IMS (Appendix L), but also results in delivering the initial PSAP capability (Task 4.1) by April 29, 2016, two months earlier than the Commonwealth's requirement. Our detailed schedule planning indicates that this accelerated schedule is achievable through the use of integration and transition activities that are executed in parallel, minimizing task interdependencies wherever possible.

Our proposed IMS includes extensive details on:

- System Design and Test Plan Development
- Laboratory Trial and Testing
- Data Center Installations and PSAP Pilot Deployment
- Phased PSAP Deployments
- Training
- Warranty and Maintenance

All tasks are inter-linked with accurate durations to provide status tracking, critical path, and identification of risks and issues. In concert with the IMS, a Work Breakdown Structure (WBS) has been developed and will be used for cost, schedule, and staffing requirements throughout the life cycle of the program.

Section 8.9, Project Management, provides additional detail.

Summary

In the following technical sections, GDIT will describe in greater detail our proposed, fully compliant solution for the MA NG9-1-1 system. We believe that GDIT's proposed solution truly represents a best value for the Commonwealth, and we look forward to working with you on this important project.

8.1.1. Scope

The State 911 Department currently provides services and equipment for approximately two hundred fifty-four (254) PSAPs throughout the Commonwealth, as well as for approximately one hundred four (104) limited secondary PSAPs, three (3) secondary PSAPs, four (4) training centers, and one (1) mobile PSAP. Primary PSAPs, regional PSAPs, and RECCs are PSAPs equipped with ALI, an enhanced 911 service capability that allows for the automatic display of information relating to the geographical location of the communication device used to place a 911 call, and ANI, an enhanced 911 service capability that allows for the automatic display of a telephone number used to place or route a 911 call, and are the first point of reception of a 911 call. A secondary PSAP is a PSAP equipped with ANI and ALI displays. It receives a 911 call only when transferred from the primary PSAP or on an alternative routing basis when calls cannot be completed to the primary PSAP. The municipalities hosting primary PSAPs, regional PSAPs, and RECCs, the number of answering positions, and trunks (wireless and wireless) are set forth on Attachment K1- Primary PSAP, Regional PSAP, and RECC Data. A list of the PSAP addresses and site survey information will be provided to bidders upon the receipt by the State 911 Department of an executed Non-Disclosure Agreement in the form attached hereto and made a part hereof as Attachment S- Non-Disclosure Agreement.

The municipalities hosting primary PSAPs, regional PSAPs, and RECCs, historical call volume (wireline, wireless, administrative line, final route), and audio monitoring points are set forth in Attachment K2- Primary PSAP, Regional PSAP, and RECC Data. There are currently approximately 6,000 certified enhanced 911 telecommunicators throughout the Commonwealth. The mobile PSAP is available 24 x 7 to respond to and temporarily replace and assist PSAPs that are rendered non-operational due to structural failure, equipment failure, infrastructure failure, or other emergency and/or pre-planned events. The mobile PSAP is deployed for training, public education, PSAP conversions and build outs, the Boston Marathon, and as an emergency backup PSAP. The State 911 Department may utilize the mobile PSAP in connection with the transition to Next Generation 911.

This RFR describes the equipment and services necessary to provide Next Generation 911 service statewide. The number and configuration of PSAPs varies from time to time at the discretion of the State 911 Department. The State 911 Department reserves the right to purchase equipment and services for new, expanded, or additional PSAP sites and answering positions, and reserves the right to change PSAP sites and/or positions during the term of the contract or any renewal thereof. The State 911 Department reserves the right to purchase equipment and services that offer additional or new functionalities offered by the system, on such pricing, terms and conditions as may be negotiated with the contractor.

No change in the cost or payment terms specifically identified within this RFR shall be warranted unless there is a material change to a regulation, guideline, standard, or order of the State 911 Department that significantly alters the contractor's ability to provide services, as determined solely in the discretion of the State 911 Department.

All purchases of hardware, software, and/or CPE necessary to fulfill the requirements of the contract, and any renewal thereof, may be made by the contractor on behalf of the State 911 Department and/or the Commonwealth if the contractor demonstrates, to the satisfaction of the State 911 Department, that procurement by the contractor of such material will achieve the best value in fulfilling the requirements of the contract, or any renewal thereof. The State 911 Department reserves the right to procure any such hardware, software, and/or CPE through a procurement vehicle other than this RFR if to do so would result in the best value in fulfilling the contract, or any renewal thereof. The contractor shall be required to install and maintain any and all such hardware, software, and/or CPE, and shall provide pricing on a per position basis to install and maintain any and all such hardware, software and/or CPE procured directly by the State 911 Department and/or the Commonwealth.

The specifications set forth in this RFR will form the basis for and be incorporated into the contract that will be executed with the contractor, and, therefore, the failure of a bidder to state in its response its inability to meet the specifications set forth in this RFR shall be deemed to constitute the acknowledgment of the ability of the bidder to comply with the specifications set forth in this RFR.

The order of precedence of the contract shall be as follows: Commonwealth Terms and Conditions, Standard Contract Form, the RFR, the bidder's response to the RFR.

GDIT will comply with the RFR specification.

8.1.2. Format of Response

Bidders shall follow the same sectional format of this RFR and provide an individual response to each RFR specification in its response. All responses shall be presented using the same numbering sequence and order used in this RFR.

Bidders shall acknowledge that the bidder accepts the terms and conditions of the RFR specification by clearly stating in the affirmative that the bidder shall "comply" with or "agree" to" the specification. Bidders are advised that a response of "understands" or "understood" may be considered non-responsive. In addition, bidders shall explain in detail how the system shall meet the requirements of the RFR, and a failure to do so may be viewed as an incomplete response.

Bidders shall include in the response a detailed list of all components required for a comprehensive solution. Bidders shall complete Attachment R1 – List of Commodities/Services indicating the components for which the bidder is submitting a response. In addition, bidders shall identify by listing on Attachment R2- List of Commodities/Services – Sub-Contractors/Other Vendors which components, if any, the bidder proposes to be provided by a subcontractor and/or another vendor. Bidders shall provide a detailed diagram of the Next Generation 911 system proposed by the bidder, identifying each of the components, their operation, and interaction and which components, if any, the bidder proposes to be provided by a subcontractor and/or another vendor.

The State 911 Department proposes a comprehensive solution for the Next Generation 911 system, and, therefore, bidders shall identify by listing on Attachment R2- List of Commodities/Services – Sub-Contractors/Other Vendors any required specifications or components that are not addressed in this RFR.

Bidders shall include a product and technology roadmap indicating future features and capabilities that are being added to each of the components of the comprehensive solution. Where possible, bidders shall include release dates for new features.

Bidders shall NOT include any information relative to costs, cost elements, or pricing in the technical response. All cost and pricing shall be addressed solely in the pricing response.

GDIT complies with specification in the RFR.

8.1.3. Alternatives

A response that fails to meet any material term or condition of the RFR, including the submission of required attachments, may be deemed unresponsive, may be disqualified, and may be rejected. Unless otherwise specified, bidders may submit responses proposing alternatives which provide equivalent, better or more cost effective performance than achievable under the stated RFR specifications. These alternatives may include related

commodities or services that may be available to enhance performance during the period of the contract. The response should describe how any alternative achieves substantially equivalent or better performance to that of the RFR specifications.

The State 911 Department will determine if a proposed alternative method of performance achieves substantially equivalent or better performance. The goal of this RFR is to provide the best value of commodities and services to achieve the procurement goals of the State 911 Department. Bidders that propose discounts, uncharged commodities and services or other benefits in addition to the RFR specifications may receive a preference or additional points under this RFR as specified.

GDIT is not proposing alternative solutions. We have included in Section 8.21 (Additional Services) some areas where we believe the Commonwealth may derive benefit from additional features or future enhancement.

8.1.4. Minimum Bid Duration

Bidders responses/bids made in response to this RFR shall remain in effect for at least one hundred eighty (180) days from the date of bid submission.

GDIT will comply with the RFR specification. This bid response will remain in effect for one hundred eighty (180) days from the date of bid submission.

8.2. COMPLIANCE WITH LAW

The contractor shall, in the performance of all services provided by the contractor, including but not limited to, equipment, installation, training, maintenance and performance services and reports comply with the requirements set forth in Section 560 of the Code of Massachusetts Regulations, Standards for Enhanced 911, as may be amended from time to time, and any and all federal, state, and local laws, regulations, rules, guidelines, standards, and orders in effect at the time of the issuance of this RFR or promulgated or issued from time to time throughout the term of the contract or any renewal thereof. The contractor shall adhere to standards and specifications as established by NENA, unless otherwise agreed to in advance in writing by the State 911 Department. All work and materials shall comply with all applicable federal, state, and local laws, municipal ordinances, regulations and direction of inspectors appointed by proper authorities having jurisdiction. The contractor shall immediately correct any and all code violations, deficiencies, or non-compliance at no cost to the State 911 Department or the Commonwealth, and the contractor shall indemnify and hold harmless the State 911 Department and the Commonwealth from and against any liability, loss, damages, or costs that either may incur as a result of the contractor's violations, deficiencies, or non-compliance, whether willful, negligent, or otherwise.

GDIT will comply with the RFR specification.

8.2.1. Standards

Bidders shall possess the required knowledge and industry participation in the products and services being proposed.

GDIT complies with the RFR specification. The GDIT team consists of NG9-1-1 industry leading organizations that participate in a variety of NG9-1-1 Industry Collaboration Event (ICE) sessions that are instrumental in developing standards and protocols as well as demonstrating industry leading functionality and integration capabilities. Our team possesses the requisite knowledge and industry participation contained within this proposal to deliver a highly reliable and industry leading NG9-1-1 solution for the Commonwealth of Massachusetts.

The State 911 Department reserves the right to reject non-standard systems that may impede the Commonwealth from participating in the larger national and international networks of Next Generation 911 technologies. Further, the contractor shall warrant compliance with known applicable standards at the time of system acceptance and shall make continual upgrades to the system as may be required to meet evolving standards for the duration of the contract.

In addition to all other standards set forth herein and in addition to all other NENA i3 standards, the system shall comply with the following standards:

- *NENA 8-003 v1 Detailed Functional and Interface Specification for the NENA i3 Solution, Stage 3 Version 1;*
- *NENA 8-002 NENA Functional and Interface Standards for Next Generation 0-1-1 Version 1.0 (i3);*
- *NENA 08-751 NENA i3 Technical Requirements Document;*
- *NENA 04-001 Section 10.4 Software Quality;*
- *NENA 58-001 NENA IP-Capable PSAP Minimum Operational Requirements Standards;*
- *NENA 58-501 IP PSAP 0-1-1 System Features and Capabilities;*
- *NENA 75-001 Security for Next Generation 0-1-1 Standard (NG-SEC), NENA 75-001 v1, and NENA 04-503 v1;*
- *NENA 75-502, NENA 04-502 v1, NENA 04-503 v1, NENA 08-506 v1, NENA 08-752 v1, NENA 71-502 v1, NENA STA-003;*
- *Applicable Internet Engineering Task Force Standards (IETF), such as IP protocols, IP routing protocols, SIP, RTP, LoST, and the PIDF-LO; and*
- *NENA Emergency Services IP Network Design for NG0-1-1. Bidders shall describe in detail in the response how they shall meet such standards in their design.*

A collaboration and partnership between the Commonwealth and the GDIT team creates a unique opportunity for the Commonwealth to help influence, evolve, and further define NENA standards and protocols based on real-world Commonwealth public safety requirements. GDIT's design complies with applicable NENA standards. Additionally, GDIT and our teammates continually align product development roadmaps to align with evolving NENA standards.

GDIT's proposed legacy gateway interconnection systems have been tested at NENA Industry Collaboration Events (ICE) and are in production with traditional telecommunications providers. From an ESInet perspective, all of our proposed equipment solution providers participate and in the development of NENA standards including alignment of product development with applicable standards including the proposed Session Border Controllers (SBC), which is widely utilized across various IP and SIP-based service providers within large global networks.

GDIT's Customer Premise Equipment (CPE) solution will *not* require any upgrade to deliver true i3 compliant NG9-1-1 capabilities. The CPE solution was built from the ground up to support i3 standards. The proposed CPE solution is the first publicly demonstrated interoperable i3 NG9-1-1 CPE capabilities three years ago in October of 2010 at the Gulf Coast NENA conference. i3 NG9-1-1 capabilities have been included in every product release starting with 2.0, the current release is version 3.1 and includes i3 capabilities today in the current shipping release.

The Security for Next-Generation 9-1-1 Standard (NG-SEC) 75-001 identifies the basic minimum security requirements applicable to NG9-1-1 Entities, and provided a basis for auditing, and assessing levels of security and risk, and an exception approval /risk acceptance process in the case of non-compliance. GDIT complies with this standard.

GDIT will also ensure alignment and compliance to applicable standards through close partnership with the Commonwealth during design development, design review, and design approval milestone gates as well as thorough testing and acceptance procedures. We are committed to ensuring interoperability with other standards based NG9-1-1 functional elements.

As thought leaders in the industry, team GDIT has members within the NENA i3 Architecture Working Group, the Policy Routing Rules Working Group, and the Security for 9-1-1 Working Group. In addition, team GDIT is an active participant in NENA's ICE events. Participation in NENA working groups and ICE events ensures team GDIT and the Commonwealth have current intelligence on the development of critical standards, and will incorporate any necessary changes and modifications into our solution as they are developed. GDIT will warrant compliance with known applicable standards at the time of system acceptance and will make continual upgrades to the system as may be required to meet evolving standards for the duration of the contract.

8.2.2. Open Standards

The system shall be based on open standards such as ITU, IEEE 802 at OSI Layer-2, and IP and TCP, as defined by the IETF in the applicable RCFs, at OSI Layer-3 and above.

Bidders shall disclose whether the system uses any proprietary standards or protocols, and bidders shall reveal any limitations on the use of open standards.

GDIT will comply with the RFR specification. Our subcontractor Emergency CallWorks (ECW) utilizes open source extensively across the software stack. The Java Enterprise web application, which provides all 9-1-1 business logic and acts essentially as our Automatic Number Identification / Automatic Location Identification (ANI/ALI) controller, is the only component that is not open source. All other software components of the system from the operating system to the SIP stack are derived from open source solutions.

The ECW product development and enhancement process is in no way limited or directed by the advances or lack of advances in third-party projects from which we derive source. The benefit to the Commonwealth in utilizing open source software is the increased flexibility and control as well as providing a cost-effective web-based CPE solution that provides industry-leading capabilities to NG9-1-1 public safety call takers. Please see Section 8.7 and specifically Section 8.7.3 (Customer Premises Equipment) for additional details of the CPE solution.

8.2.2.1. Special Equipment

Bidders shall state whether the system will require any non-traditional (i.e., special purpose) equipment to be located at a PSAP and/or a data center.

GDIT complies with the RFR specification. A device that could be considered "non-traditional" within the PSAP is the Emergency CallWorks Audio Interface Unit (AIU) that provides – if required – headset integration and switching between telephone and radio. The Emergency CallWorks AIU does connect via standard interfaces including IP over powered Ethernet. This piece of equipment is produced by ECW because there is no comparable product available on the open market.

The proposed design does not require any additional "non-traditional" equipment within the data center or PSAP.

8.2.3. Facilitating Transition

Bidders shall describe how the system shall be configured to support the transition from legacy call handling to Next Generation 911 call handling.

GDIT will comply with the RFR specification. For details on the full transition approach, please see Section 8.13, Migration, Deployment, and Installation. The GDIT team, as discussed throughout this proposal, believes strongly in approaching this program in phases, commensurate

with the stages defined by the Commonwealth and paired with our team's extensive experience migrating clients from legacy infrastructures to advanced, enterprise technology domains. As part of the solution, GDIT is bidding a full-time Transition/Migration Liaison who will focus solely on the transitioning of i3 NG9-1-1 services into production with a resolute "Do No Harm" philosophy to ensure ongoing legacy and new i3 operations are not adversely affected. Through our direct and relevant experience in undertakings of this size, scale, complexity, and criticality, GDIT brings the requisite discipline, control, risk mitigation, and organizational subject matter expertise that is pertinent to this program's success.

The MA NG9-1-1 project is one that utilizes multiple cores, disparate assets, integrated technologies, and an intricate transition process that demands large, complex project experience from a Large Systems Integrator (LSI). GDIT is that LSI, our experience is global, our name synonymous with "mission critical," and our plan for the Commonwealth is specifically tailored based on our team's expertise and involvement in NG9-1-1 initiatives since i3 was first conceptualized.

Transition planning will *first-and-foremost* ensure a "Do No Harm" safeguard approach to current operations.

Configurations to support the transition from legacy call handling to NG9-1-1 call handling will go through rigorous testing and acceptance in partnership with the Commonwealth at GDIT's i3 Solutions Interoperability Lab, located in Needham, MA. Legacy to NG9-1-1 call handling configurations will then be tested and accepted on non-production call handling circuits within the data centers (ESInets). This testing acceptance process will include additional procedures to not only test transition from legacy to NG9-1-1 call handling, but also test call survivability and failover capabilities once the call handling has transitioned from legacy to NG9-1-1. GDIT will apply proven program management and change management best practices per the Commonwealth's "CommonWay" project management principles to ensure tested and accepted configurations are documented and incorporated into a configuration baseline to ensure successful transition into the production environment. A detailed description of the transition from legacy call handling to the NG9-1-1 system is provided in Section 8.7.12 (Location Information Service Interface) and Section 8.7.13 (ALI Database Services) of this proposal. The following system builds and testing will occur separate from ongoing operations:

- GDIT NG9-1-1 Laboratory staging and testing including simulated PSAP position.
- Move, install, and test data center systems.
- Build and connect ESInet WAN Core, and backhaul connectivity between data centers.
- Build connections to all carriers to allow ingress emergency services traffic to both data centers. Test circuits into ESInet.
- Build individual PSAP ESInet WAN connectivity (e.g., access loop) to support migration schedule.
- Build internal PSAP internal networking environment, testing connectivity to data centers. PSAP IP network equipment instantiation (aligned with Milestone 4).

- Build/deploy NG9-1-1 call taker workstations, test to ESInet routing and configuration in parallel with operational E9-1-1 call taker consoles.
- Perform cutover of legacy CAMA trunks for individual PSAP, by migrating carrier routing from terminating at PSAP to terminating at data center.
- Test live operation; perform roll-back if required.

This approach to parallel system configurations and testing will ensure all environments are ready for transition into production while ensuring no interruption to ongoing operations occurs.

Detailed Migration Plan

The contractor shall propose a detailed plan for and shall facilitate the migration of 911 services from the legacy system to the Next Generation 911 system at all interfaces between the contractor and other emergency call originating communication service providers in order to accomplish 911 call delivery that meets the quality, reliability, and availability requirements of this RFR. This includes, but is not limited to, stating the terms, conditions, procedures, and processes for interconnection and exchange of information between other carriers' networks and systems and the contractor's system, and includes interfaces that shall allow for the means to timely exchange information such as legacy ALI database updates, PS/ALI services, exchange of monitoring and trouble ticket information, trunk connections to the legacy network gateway, and IP connections to border control functions.

GDIT's Integrated Master Schedule (IMS) includes detailed transition and migration tasks required for the project and is included in Appendix L. After award, the GDIT team will work with the Commonwealth to review and finalize this schedule. Section 8.7 (Next Generation 9-1-1 Architecture) and Section 8.13 (Migration, Deployment, and Installation) provide further details on our migration plan.

Monitor All Ports on Border Control Functions

The contractor shall monitor all ports, inbound and outbound, on the border control functions.

The Oracle's Session Border Controller (SBC), formerly known as Acme Packet, is GDIT's Border Control Function (BCF) element and runs on the same set of software and hardware deployed for many years. Oracle's BCF management platform, Palladion, is part of our solution and will be utilized to monitor all ports, inbound and outbound, on the BCF. The BCF currently runs live mission-critical calls for various global organizations. Large service providers, financial institutions, and government agencies utilize these base products. GDIT and our teammates have assisted many organizations in their transition from legacy PSTN to IP multimedia unified communications solutions and will monitor all ports, inbound and outbound, on the BCF. Please see Section 8.7.5 (Border Control Function) for more information on the proposed BCF.

Work Closely with Communication Service Providers

The contractor shall, as necessary, work closely with communication service providers and shall cooperate fully with them in order to accomplish a successful transition to the Next Generation 911 system.

GDIT regularly works with service providers to ensure smooth transition and delivery of networks and systems. In some instances, we act as the government's agent. GDIT will work closely with communication service providers and cooperate fully with them in order to accomplish a successful transition to the NG9-1-1 system.

8.3. ESINET

The contractor shall provide, design, monitor, manage, and operate the network, including the supply of all network equipment and all network services and connection required to create a fully functional and compliant Next Generation 911 system.

The network links shall include a mix of private (Commonwealth-provided) and public (commercial carrier) facilities. While the network facilities may be obtained from more than one source, the contractor shall operate and manage the network as a single network from the perspective of the State 911 Department.

The public (commercial carrier) facilities will be the primary path, and the private (Commonwealth-provided) facilities where available shall be the secondary path for failover where practical. The private network facilities shall include the Massachusetts Broadband Initiative (MBI) deployment currently being installed in western Massachusetts and other network assets to be identified by the State 911 Department. The State 911 Department requires that the contractor shall make use of the private network assets identified by the State 911 Department. The currently available private (Commonwealth-provided) network assets are identified on Attachment T-Commonwealth Network Assets attached hereto and made a part hereof. The contractor may be required to coordinate with third parties, including without limitation, network operators and contractors associated with the MBI project. As the Commonwealth deploys more private network facilities, the State 911 Department may require that the contractor migrate carrier-based services to these private facilities, and the contractor shall do all things and take all action necessary to migrate such services at the direction of the State 911 Department.

GDIT will comply with the RFR specification.

GDIT is fully committed to and will provide all network equipment and services required to create a fully functional and compliant NG9-1-1 system.

GDIT is proposing a true next generation and NENA-compliant solution that is designed and built for IP-based call routing and includes the systems and databases required in a transitional environment. The solution allows for enhanced call routing and delivery, as well as the ability to reroute calls to any PSAP, both within and outside the Emergency Services IP Network (ESInet).

GDIT fully concurs with and supports designing the ESInet using a mix of Commonwealth's network and GDIT-provided public network assets. We also believe mixing private and public assets will provide the best value to the Commonwealth and allow additional redundancy and diversity for the critical ESInet. GDIT will fully collaborate and coordinate with the Commonwealth and third parties, such as network operators and MBI contractors. Additionally, we will fully cooperate and migrate carrier-based services to private facilities as directed by the Commonwealth to provide the value network design and connectivity. Upon establishment of the ESInet, GDIT will operate, monitor, and manage the network as a single network from the perspective of the State 911 Department.

Specifically, our ESInet solution is designed with a geographically diverse redundant core architecture that ensures continuous system operation for virtually any contingency as well as absorbing the impact of a major network outage or a catastrophic event to one of the locations. Our ESInet IP network design ensures a systemic and end-to-end managed network that enables shared applications and the ability to replicate E9-1-1 features and functions to improve access to emergency services for callers and significantly advance the Commonwealth's effectiveness and efficiency for emergency communications and response.

As NENA and other governing standards continue to be developed, our ESInet design allows he Commonwealth to take full advantage of the i3 vision as it becomes commercially available. Our core NG9-1-1 architecture and infrastructure remains in place while newly available components

and software elements can be easily added or upgraded without disrupting services or complete replacement, allowing it to easily meet the demands of the future.

Our ESInet system design, combined with our fully thought out migration strategy and know-how, will assure migrating to next-generation in a logical, smooth, and cost-effective manner.

GDIT's NG9-1-1 technology solution implements a multi-vendor, standards-based approach to include all products and services necessary to deliver program success. Our aggregate team represents the technology leaders in standards and interoperability, including critical roles in the NENA working groups, participation in the NENA ICE events, and testing in the GDIT i3 Solutions Interoperability Lab. We categorize the primary technology elements of our solution as:

- **NG9-1-1 Data Centers:** Build two (2) 'hosted', high-availability, and mirrored data centers (with an optional third data center) that receive ingress (public safety) traffic from all carriers, and provide comprehensive and centralized NG9-1-1 applications and i3 traffic routing to call takers.
- **Carrier Interface:** Provide coordination and termination of carrier ingress traffic for public safety service requests. Support initial 'transitional' architecture using legacy interfaces and private location databases, and migration to the i3 end state.
- **ESInet WAN:** Build a 'composite' ESInet Wide Area Network (WAN) using a mix of private and leased assets that connects the data centers to all remote locations (PSAPs and training centers) with redundancy and performance assurance that ensures delivery of NG9-1-1 payloads to call taker positions.
- **PSAP Modernization**: Modernize existing PSAP systems to enable delivery of NG9-1-1 traffic, payloads, and methodologies, leveraging Voice over internet Protocol (VoIP) and providing integration with legacy peripheral systems and processes. Ensure user adoption and minimize any operational impact.
- **Network Operations:** Build a centralized network and security operations capability that allows for systemic proactive and reactive operations, administration, maintenance, and provisioning that assures the highest reliability, control, and visibility of services and integrity of data.

The ESInet WAN represents the majority of required telecommunications services in GDIT's proposed solution, needed to support the centralized 'hosted' application model. With carriers sending (public) ingress traffic to each data center, the ESInet WAN supports distribution of traffic between data centers and (primarily) PSAPs. The ESInet WAN is composed of two primary components: the WAN Core and Access loops. The WAN Core is a high-capacity, highly redundant, high-performance, and fully managed MPLS mesh utilizing our teammate, Windstream. Within Massachusetts, Windstream has built their core using both privately owned and leased facilities from diverse partners – maximizing route diversity, fiber utilization, and carrier diversity. The core networking is enabled by a highly redundant Cisco MPLS networking environment in a full 'carrier-class' architecture, assuring 99.999% reliable transport.

The Windstream core is also fully monitored and managed to maximize continuous understanding of the health and performance of the transport network. Proactive maintenance ensures awareness of both hard (system and facility failure) and soft (congestion, degraded performance) conditions that could potentially affect active or future services. Intelligent systems support WAN core rerouting decisions based on established Service-Level Agreements (SLAs). The GDIT NSOC will interface directly with Windstream to build transport awareness into our comprehensive monitoring construct, ensuring visibility and remediation from the transport layer to the application layer. GDIT also highlights that Windstream and GDIT have agreed to share a demarcation device at all remote locations, eliminating back-to-back routers that are typically required for ownership separation. Removing this demarcation 'stacking' reduces points of failure, reduces service costs, improves speed of fault location, and supports SLA management.

Access loops provide the 'last mile' connection between the ESInet WAN Core and individual sites, and are typically contracted across multiple carriers. Considerations in selecting access loops include:

- Carriers having physical media existing to the site
- Media type to support performance SLA and availability
- Ability and agreement to meet established performance and availability SLAs and bandwidth demands
- Availability of multiple connections
- Availability of dual building access
- Availability for network-network interface (interconnect) with the Core
- Cost

GDIT complies fully with the defined a set of requirements for primary, secondary, and optional tertiary connections that have been included in GDIT's proposal. In most cases, due to availability, primary access loops will be provided by Verizon, using single or multiple existing T1 (copper) circuits to achieve the necessary bandwidth requirements. Windstream has several NNI established with Verizon across the Commonwealth, with exceptional operational interworking with Verizon to order, test, manage, and maintain circuits, greatly assisting in improving schedule pressures. Larger sites (as identified) will utilize Windstream direct Metro Ethernet fiber connectivity, providing redundant and scalable direct access to the Windstream Core. Figure 10 illustrates the individual components of the ESInet WAN.

Secondary connections have been proposed to offer carrier and circuit redundancy to each site. It is expected that the Commonwealth will consider the use of existing or future Massachusetts Broadband Initiative (MBI) circuits where available. Windstream has an existing Network-to-Network Interface (NNI) with the Axia/Massachusetts Broadband Initiative, which allows traffic to access the ESInet WAN Core without the use of the public Internet and supporting traffic engineering to implement performance SLAs. Windstream is also working with Axia and the Commonwealth on other network initiatives, including CapeNet, MassNet, and FirstNet, which may offer additional options for access loops, and further improving utilization of available

Commonwealth assets. The GDIT team will work in partnership with the Commonwealth to evaluate the use of all networks as primary or secondary connections as they become available.

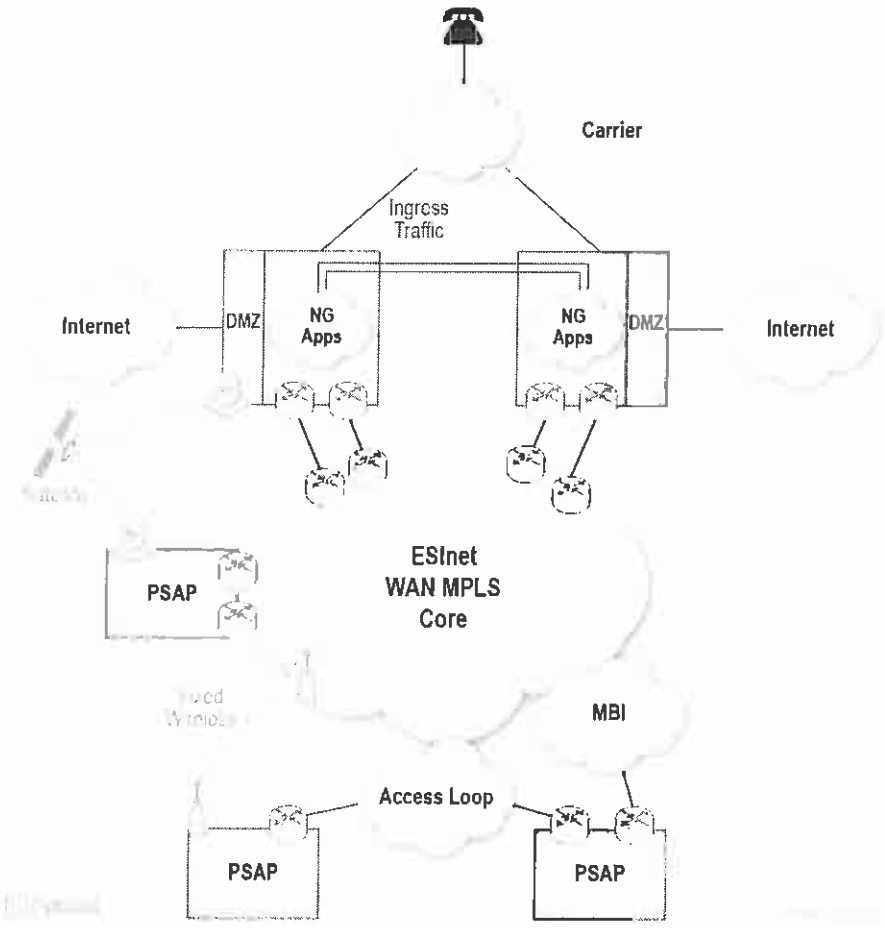


Figure 10. Telecommunication Services

Specifically for Boston Police and Boston Fire, GDIT's proposed solution provides secondary connectivity utilizing Windstream Fixed Wireless to augment the primary redundant Metro Ethernet connections. Fixed Wireless is a broadband transport solution that uses an Federal Communications Commission (FCC) licensed wireless spectrum to provide connectivity between two locations (point-to-point). Windstream presently has line-of-site access from existing systems, located on the Prudential Center, to each facility with direct access to the Windstream Core network. These facilities provide 20 MB of symmetrical bandwidth and fully support the established packet performance and SLAs established by the Commonwealth to achieve quality of service and availability, with exceptional cost value. Further, the wireless traffic utilizes encryption technology that ensures privacy and security, and supports multiple circuits over a single transport system, allowing voice and data applications to be served in a converged fashion. Additional fixed wireless routes may be available in the future to support other PSAPs, upon request and agreement with the Commonwealth.

Tertiary connections to several of the larger PSAPs are provided utilizing a third carrier with a fully separate network to provide wired connectivity. Optional tertiary connections have been provided to all sites with six or more call taker positions utilizing satellite connectivity. An overview of the proposed tertiary technologies is as follows:

- **Satellite**: Hughes Network Systems has provided a satellite solution capable of covering all sites in the proposed NG9-1-1 solution. The design utilizes a small (1.2 meter) antenna at each PSAP site to provide up to 2.0 MB connection to a shared connection at each data center. Each data center base station will support up to 8 MB of connections for individual PSAPs. Hughes leverages the SPACEWAY-3 satellite, which has onboard processing capability to allow data and voice to be routed directly between any two locations, without the need to traverse a ground hub. This feature provides better SLA performance than most satellite connections, supporting greater than 3.0 for Mean Opinion Score (MOS) on voice circuits. Specific engineering on bandwidth would be required to identify the number of simultaneous calls within a Constant Bit Rate (CBR) construct.

In all but a few cases, the access loops will deliver traffic to the ESInet WAN Core through established NNI, funneling all traffic through the identified data center connection points to enable network and security monitoring, SLA management, and data center routing diversity. Each data center will also enable Internet connections through established perimeter network – referred to as the Demilitarized Zone (DMZ) – leveraging appropriate security and authentication. Public Internet access (through the DMZ) will initially support, at minimum, the mobile PSAP, but can be expanded to include other off-network connectivity, such as home-based workers. 20 Mb connections are provided initially and can be optionally expanded to support undefined access demands.

Other telecommunication services provided in GDIT's proposed solution include:

- Off-network (PSTN) SIP trunks, provided at each data center to support inbound/outbound calling from each call taker position. This administrative calling alternative allows integration of off-net calling directly with the call taker workstation (point and click), for such activities as abandoned call callback. On-net station-to-station calling is also supported in this function, and all activities are included in logging, recording activity reporting.

- Termination of (Commonwealth-provided) local PSTN trunks and existing telephone numbers at each PSAP for inbound/outbound calling using the PSTN (e.g., one- and two-way). GDIT's proposal includes the Cisco CallManager survivable voice gateway function with analog cards in each edge router to enable PSTN administrative calling even if the ESInet connections are not functional.

- Delivery of a private and redundant 10G connection (wavelength service) between data centers that supports synchronization of databases and applications, replication of data, and survivability of applications and/or ESInet WAN data center connections.

8.3.1. Network Design

Bidders shall submit with the response a proposed network design and network diagram, including overall architecture, bandwidth requirements, QoS requirements, and any required protocols, for the Next Generation 911 system. The design for the proposed network shall provide sufficient detail for the State 911 Department to

determine the bidder's expertise in designing a highly redundant and diverse network, and bidders shall provide as much detail as possible to allow the State 911 Department to properly evaluate the response. The network diagram shall display sufficiently detailed information regarding the core network and each site connection so that the topology and design are clear. The network diagram and narrative shall provide sufficient detail so that technical reviewers can identify how the design meets the requirements of this RFR and shall clearly display, at a minimum, the following:

- *Physical topology;*
- *Diversity in topology;*
- *Non-diverse network segments;*
- *All known entities and all known connection types;*
- *Secondary and tertiary technologies with interfaces to master topology;*
- *Rings;*
- *Circuits;*
- *Interconnection and aggregation points;*
- *Load balancing capability;*
- *Approach to meeting availability requirements; and*
- *Data Center connections.*

As soon as possible following contract award, but in no event later than sixty (60) days following contract award, the contractor shall submit to the State 911 Department for approval a proposed detailed network design and technical documents for the Next Generation 911 system that shall incorporate the IP addressing, routing, QoS, traffic engineering, proposed carriers for each link, and a detailed analysis indicating how the network shall support the full traffic load, availability, and other requirements set forth in the RFR.

The detailed network design shall incorporate all entities and all connection types, including but not limited to, connections to PSAPs, connections between data centers, connections to the public Internet, connections to communications service providers, via traditional trunks and private IP circuits, connections to legacy PSAPs, connections to existing selective routers; and any other connections that may be required. The final network design shall be subject to the approval of the State 911 Department.

The network shall be a high performance network based on current industry and NENA i3 standards, protocols and technologies. The primary network technology shall be a mix of MPLS, carrier Ethernet, or other i3 transport standards. QoS features shall be provided, and PSAPs shall have dedicated bandwidth to eliminate contention.

The network shall be designed and configured to support many payloads, including voice, data, and multi-media. The network shall be able to identify, prioritize and route/re-route traffic based on data type, application, origination point, destination point, and other parameters. In particular, the network shall be able to identify and prioritize voice calls and maintain a mean opinion score of 4.0 or above. QoS features shall be deployed for this purpose.

The network shall accommodate growth of bandwidth requirements, interconnection to additional sites, and interconnection to national or other state ESInets in the future. The network shall support such future growth and interconnections with minimum impact on the infrastructure through incremental additions to the existing network.

The network shall be based on open standards. The overall design shall scale with respect to bandwidth, additional sites, and interconnection with other ESInets. The network shall incorporate facility and equipment diversity. The State 911 Department has a preference for physical or route diversity over logical or equipment diversity where feasible. In certain cases, diverse wireline carriers may be required for PSAPs, as determined by the State 911 Department. At a minimum, the contractor shall provide diverse entries for PSAPs with six (6) or more positions. The contractor shall also provide diverse entries for all other PSAPs identified by the State 911 Department. The contractor shall notify the State 911 Department in advance of any and all circuit or carrier changes that could affect diversity, performance, availability, or reliability, and any and all such changes shall be subject to the prior written approval of the State 911 Department.

In addition to the State 911 Department's plans to require alternate wireline carriers for certain PSAPs, bidders shall assess the use of microwave and satellite and wireless as tertiary paths. Bidders shall address the advantages

and disadvantages of each of these means as an alternate path. To the extent that the bidder concludes that the use of these means is viable as a tertiary path, such means shall be incorporated in the detailed network design and technical design documents, as directed by the State 911 Department. In certain cases, where it is not feasible to connect by diverse wireline carriers, the PSAP may be connected with microwave or satellite or wireless links, in order to provide these redundant connections. The State 911 Department expects that a switchover from a failed or degraded network to a secondary or tertiary network shall result in minimal or no data loss.

The network shall be designed so that it shall provide for 100% of all 911 payloads to be delivered to a PSAP. The network architecture design shall address network upgrades and maintenance, down time disclosures, service level agreements (that address, at a minimum, packet latency, packet loss, jitter, and quality of service), and other necessary elements.

GDIT will comply with the RFR requirements.

GDIT proposes a turn-key NG9-1-1 solution to meet the requirements of the Commonwealth's requirements, to include comprehensive engineering, installation, testing, and migration of emergency services from an E9-1-1 environment at all identified locations. Our networking solution is fully NENA compliant, and it leverages established industry best practices to deliver a high-performance, scalable solution that meets today's services demands and the service payloads of the future. Within 60 days of award, GDIT will provide and submit for approval a comprehensive set of engineering design documents that fully identify all aspects of the network design, including (at minimum) IP addressing, routing schema, traffic engineering, and all connectivity characteristics for the ESInet and ingress traffic. This design document will also document key identified behavior characteristics of the holistic design, including all redundancy and failover, QoS metrics, Service-Level Agreements (SLAs), NG9-1-1 routing, and routing between the NG9-1-1 and E9-1-1 environments.

Topology Diversity

As stated previously, GDIT will fully collaborate and work closely with the Commonwealth in selecting and designing the best value network design that could be a mix of Commonwealth's network and GDIT-provided public network assets that will provide the best-case physical diversity to ensure continuous system operation for virtually any contingency as well as absorbing the impact of a major network outage or a catastrophic event to one of the locations.

GDIT's proposed solution is designed with extensive physical topology diversity that is both separate from application layer redundancy and responsive to application layer redundancy. Physical topology diversity is achieved by first providing two (optionally three) existing Tier 3 geographically diverse data centers (Andover and Springfield Technology Park). Each data center will have three primary connectivity paths:

- Connectivity to carriers for receiving emergency service requests from the PSTN for distribution to PSAPs through the ESInet (e.g., ingress traffic). All carrier ingress traffic will be set to all data centers. These carrier connections also allow the transfer (bridging) of service from the ESInet back to the PSTN and/or E9-1-1 PSAPs, using the legacy gateways in a 'transitional' (e.g., non-i3 end state) model.

- ESInet WAN connectivity between all data centers and all PSAPs to allow for distribution of ingress traffic via the NENA-compliant geo-spatial routing construct the data centers. These connections for the ESInet WAN use a composite of private and leased services. The ESInet connections also support secondary path connectivity between data centers for replication and synchronization of ESInet applications and databases.

- Each data center will be connected to a shared private backhaul circuit to offer primary path replication and synchronization of applications and databases between data centers, and to offer rerouting of traffic from the ESInet should the ESInet (redundant) connections to the data center be down, offering network survivability as an option to application survivability.

Ingress Traffic

Ingress traffic will be provided through interconnections at each data center and each carrier. The types of connections and how these connections terminate into the ESInet are addressed in two constructs:

- Initially, and prior to carriers supporting the end-state NG9-1-1 model, utilizing a 'transitional' model relying on each carrier's ability and willingness to connect to each data center using the selective router and/or using TDM or IP direct data center connectivity. Further detail on how this transitional environment is supported is provided in Section 8.7.1, Routing Requests. These ingress connections are expected to be the responsibility of each carrier, much like their present responsibility to deliver traffic to the selective router in the E9-1-1 construct.

- In an NG9-1-1 end-state methodology, utilizing IP connectivity to each data center with location information delivered to the ESInet in the SIP headers in the NG9-1-1 format.

The proposed systems, software, and licenses within our solution fully support both of these models initially, but only expect the transitional model in the initial deployment. As such, GDIT's transitional design includes all legacy gateways and 'private' location databases to include civic or geodesic location information to the NG9-1-1 routing environment. These transitional components will be redundant between data centers, accepting all ingress traffic at all data centers. The behavior of ingress traffic in response to a system or circuit failure is dependent on the type of connections delivered, including:

- CAMA trunks sent directly from the selective router (SR) offer the least redundancy or intelligent routing of traffic. In this model, CAMA would be duplicated and sent to both data centers and terminated at TDM gateways. Failure of the primary path would require the duplicated circuit in the alternate data center, with loss of the active call. GDIT has included interfaces in our solution to terminate 25% of all traffic in this model, but expects that appropriate carrier cooperation will make it unnecessary. A variation of this model is to terminate the CAMA at the SR locations and transport them in one of the other manners (described below). This alternate option requires a termination point (placement of the PIFs) at the SR or other location, and agreement of the incumbent carrier. It is GDIT's understanding that Verizon has indicated in public forums that they will allow and support this model.

- Direct TDM connectivity to each carrier will bypass the SR completely and allow each carrier to terminate emergency services traffic directly to the data centers. The connectivity types in doing this include T1 and SS7. The gateways terminating these circuits are fully service aware of traffic/connection health and provide the immediate failover of gateways should the circuit, PIF or interface fail. GDIT has included capacity

to terminate 75% of all traffic in this manner at each data center, and we expect that most carriers will support this model initially.

- Direct IP connectivity will be similar to direct TDM connectivity, but it offers the benefits of bypassing the PIF gateways, enabling the duplication of traffic to multiple data centers and the simplicity of traffic backhaul. Without the need to deploy TDM gateways (PIFs), this traffic is terminated directly at the BCF as in the end-state architecture. The difference between the end-state and the transitional construct, however, is that this traffic does not include i3 location in the SIP headers, and must have location information (PIDF-LO) inserted by the transitional environment. GDIT's solution supports 100% of all ingress traffic terminating to the BCF in either or both the non-i3 and i3 format.

Additional connectivity paths will be provided at each data center as identified in Section 8.3 of our proposal, including Internet access, off-network administrative calling, and network and security management connectivity. Failure of any one connection path will be supported by the other data center. GDIT will notify the State 911 Department in advance of any and all changes to carrier circuits that have an impact on diversity, performance, or reliability, and we will gain written approval for identified changes.

ESInet WAN

As detailed in Section 8.3 (ESInet), the ESInet WAN will allow distribution of public safety traffic, routed per the NG9-1-1 construct within each data center, to individual PSAPs and call taker positions. Each data center will have dual and carrier-diverse 1 GB circuits connecting to the ESInet WAN, with each connection served from physically diverse central offices and using diverse carrier loops. Each central office is a carrier hotel with diverse carrier entrance facilities and backup power generators, and connects to the Windstream Core network. The Eastern Massachusetts offices serving Local Access Transport Area (LATA) 128 are Boston and Westborough, and the Western Massachusetts offices serving LATA 126 are Boston and Albany. Each data center connection is capable of supporting the entire ESInet requirements to of each data center, even if the data center is supporting the entire demands of the Commonwealth. Under typical conditions, traffic will be load balanced between the dual connections.

Figure 12 illustrates the redundant, physically diverse, and carrier-diverse design that has been developed for the Commonwealth's NG9-1-1 solution.

It is important to note that although both data centers will utilize the Boston Central Office, the circuits would come into the central office on diverse carriers and terminate into diverse Provider Edge (PE) routers. These PE routers are then supported by dual-core routers to provide a fully meshed, redundant, and resilient NG9-1-1 ESInet solution.

Data Center Backhaul

GDIT's proposed solution provides a 10 GB private backhaul connection shared between all data centers to provide two primary functions:

- To allow for data center replication and synchronization of applications, storage, database, and configurations such that each data center remains aware and ready to perform application-level survivability. This traffic can also traverse the ESInet for alternate path.

- To allow for network survivability in the event of circuit failures to a data center. In this case, Border Gateway Protocol (BGP) routing will allow for rerouting of traffic without the need for application-level survivability.

The backhaul connection is a fully redundant, physically diverse 10 GB Layer 2 connection transported as a lambda service terminating at each data center. Figure 11 provides an aerial photo for circuit paths connecting the Andover and Springfield data centers.

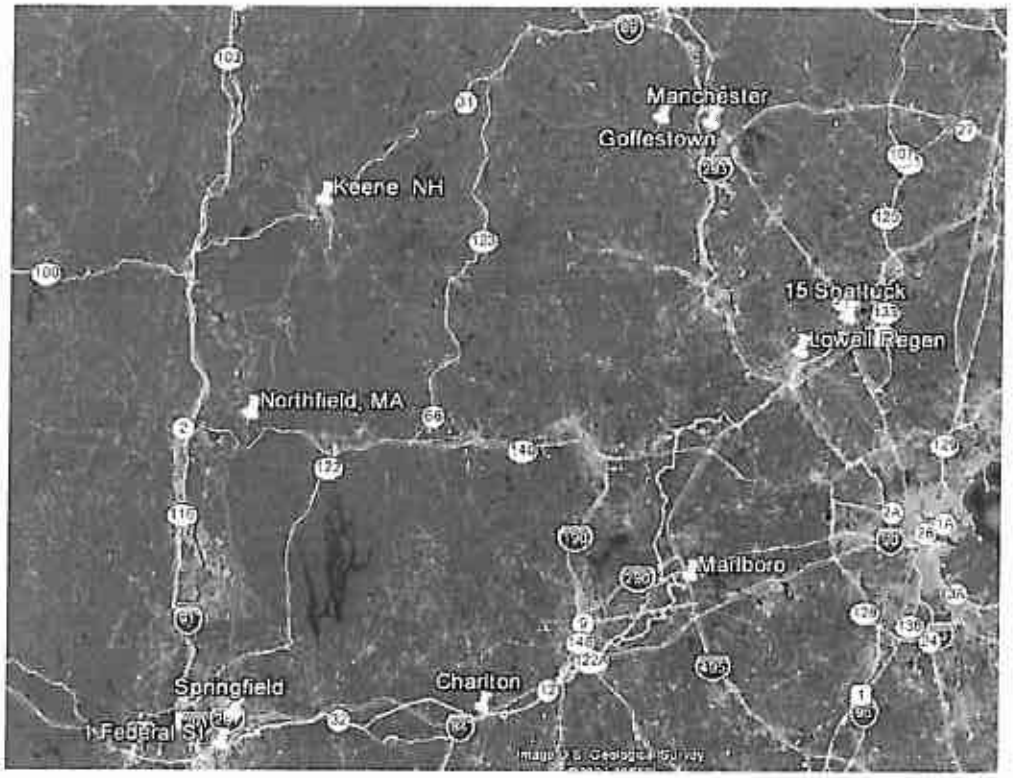


Figure 11. Aerial View of Fiber Diversity between Data Centers

Route 1 (green line in the diagram) originates at the 1 Federal Street Data Center and routes east to Marlborough, MA then north to Lowell, MA and terminating into the Andover Data Center located at 15 Shattuck Road, Andover, MA. Route 2 (red line in the diagram) originates at the 1 Federal Street Data Center and routes north through Keene, NH then east to Manchester, NH and then south before terminating into the Andover Data Center at 15 Shattuck Road, Andover, MA.

GDIT's proposed solution also considers the interconnection of other networks into the services environment, including connections to other public safety networks such as FirstNet. Initially, all other network connections will be treated as untrusted traffic, and enter the ESInet through the DMZ, where appropriate measures can be implemented for security. In the future, once the nature of connections to other networks is established, more trusted networks may be moved to dedicated termination points that leverage network-specific traffic management and monitoring. All traffic destined to the ESInet from the carriers, from other networks, or from the DMZ, will be routed and enter the ESInet through the BCF, as specified by NENA standards.

Again, GDIT will, together with the Commonwealth, further discuss and evaluate the Commonwealth's private network assets – including the Commonwealth's data centers – and we will design the best value ESInet to ensure continuous system operation even during a major or a catastrophic network failure.

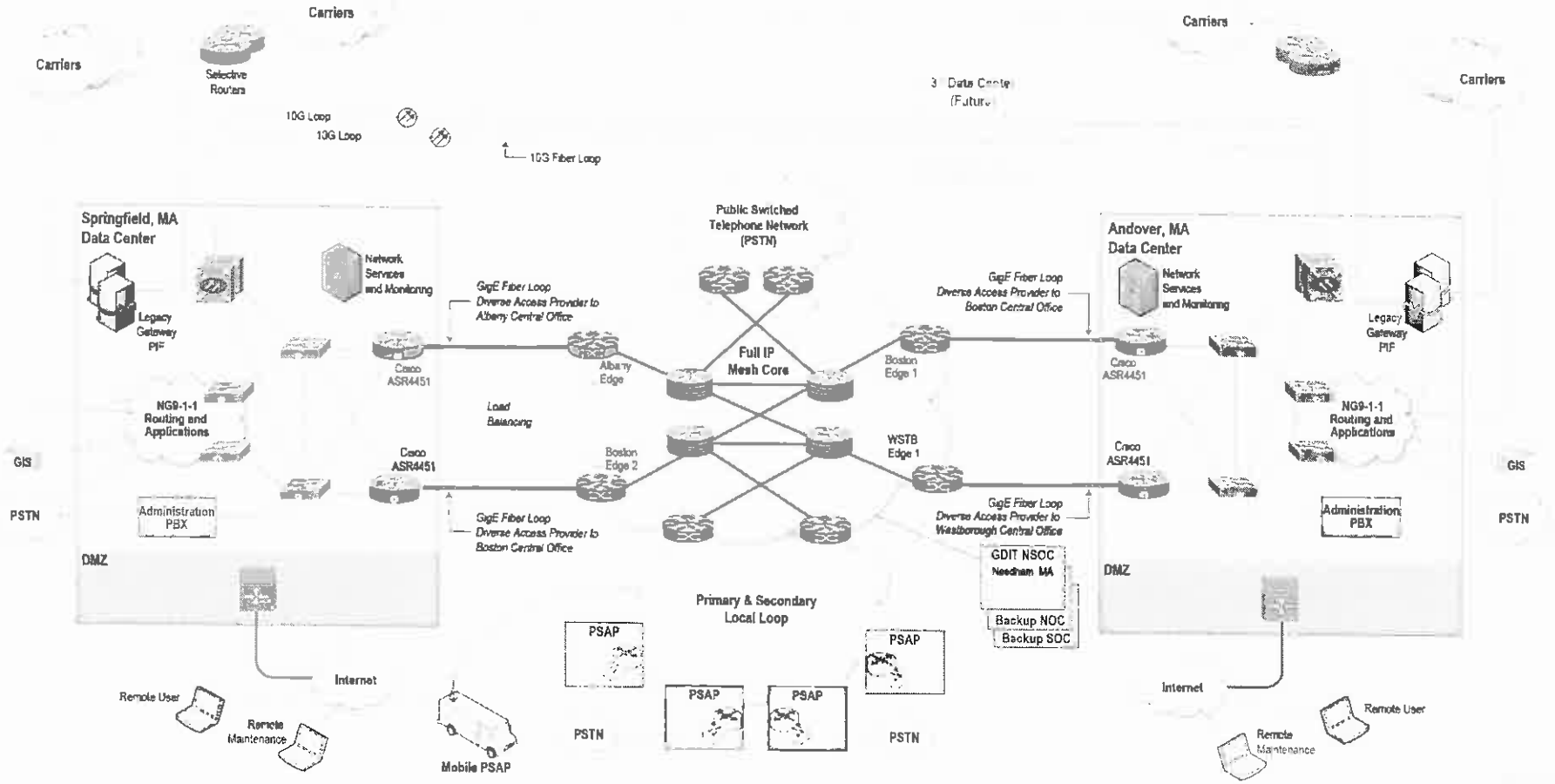


Figure 12. Diverse and Redundant ESInet Design

8.3.2. System Networking Requirements

Bidders shall identify and describe in detail all networking requirements necessary for the ideal operation of the system, including minimum and optimal bandwidth requirements, and required or preferred network protocols for Layers 1 through 4 of the OSI model.

Handoffs to the contractor's equipment from any Commonwealth-supplied ESInet will be either copper (Ethernet, RJ45) or fiber, depending on the speed or type of the connection.

GDIT will comply with the RFR requirements.

GDIT's proposed solution utilizes Cisco networking devices at all locations, with the specific model and capabilities of the device(s) selected based on the initial and expected end-state demands of each individual site. At all sites, the Cisco edge router serves a critical demarcation point for all provided ESInet WAN (primary, secondary, and tertiary) and internal LAN connections, providing end-to-end management of all traffic across WAN for security and Quality of Service (QoS). Ingress traffic is treated as untrusted, and subject to security inspection (intrusion detection, statefull firewall, etc.). Egress traffic from the site is treated to traffic engineering for secure and QoS (L3 VPN, ToS, Diffserve, etc.), with use of secondary or tertiary network based on awareness of network performance and health. All traffic (in and out) is also passively monitored and reported for enhanced, real-time, and historical understanding of service quality, security, and event detail reporting.

ESInet WAN Networking

NENA standards define the enablement of a secure, resilient, and assured service ESInet WAN connectivity between all sites utilizing MPLS and/or Layer 3 VPN tunnels. Where both methodologies are supported by GDIT's solution, we believe an L3 VPN implementation and a combination of internal and external Boarder Gateway Protocol (i.e., BGP) offers operational simplicity and increased ability to locate faults and/or performance issues. This choice is further supported by the predominant traffic flow between the data centers and individual PSAPs, and little traffic between PSAPs. GDIT's proposed network topology is based upon L3 GRE using Dynamic Multipoint VPN architecture, with traffic encrypted at the edge. In this design:

- Each Customer Edge Router (CER) will be configured to peer with a service provider router using External Border Gateway Protocol (EBGP) so that each router in the mesh can learn routes for the distant end to establish the IPsec VPN tunnels.
- Data center and PSAP internal networks will be advertised between sites with the IPsec tunnels via EBGP using a private autonomous system numbers, IP addresses will not be advertised or be accessed from non-ESInet IP networks.

Benefits of the dynamic VPN architecture include:

- Provides instantaneous, any-to-any IP connectivity using a group IPsec security policies.
- VPNs are dynamic; IPsec tunnels are established when needed.
- Unlike traditional IPsec point-to-point VPN tunnels in a full-mesh architecture, Group VPN does not require provisioning a complex connectivity mesh.
- Has lower hardware processor and memory requirements.

- Easier to manage, provision, and troubleshoot.
- Dynamic VPN preserves the IP source and destination addresses during the IPsec encryption and encapsulation process, integrates very well with QoS and traffic engineering.

This network design was chosen for security, reliability, operational maintainability, and ease in troubleshooting. Figure 13 represents the routed connections across the ESInet WAN.

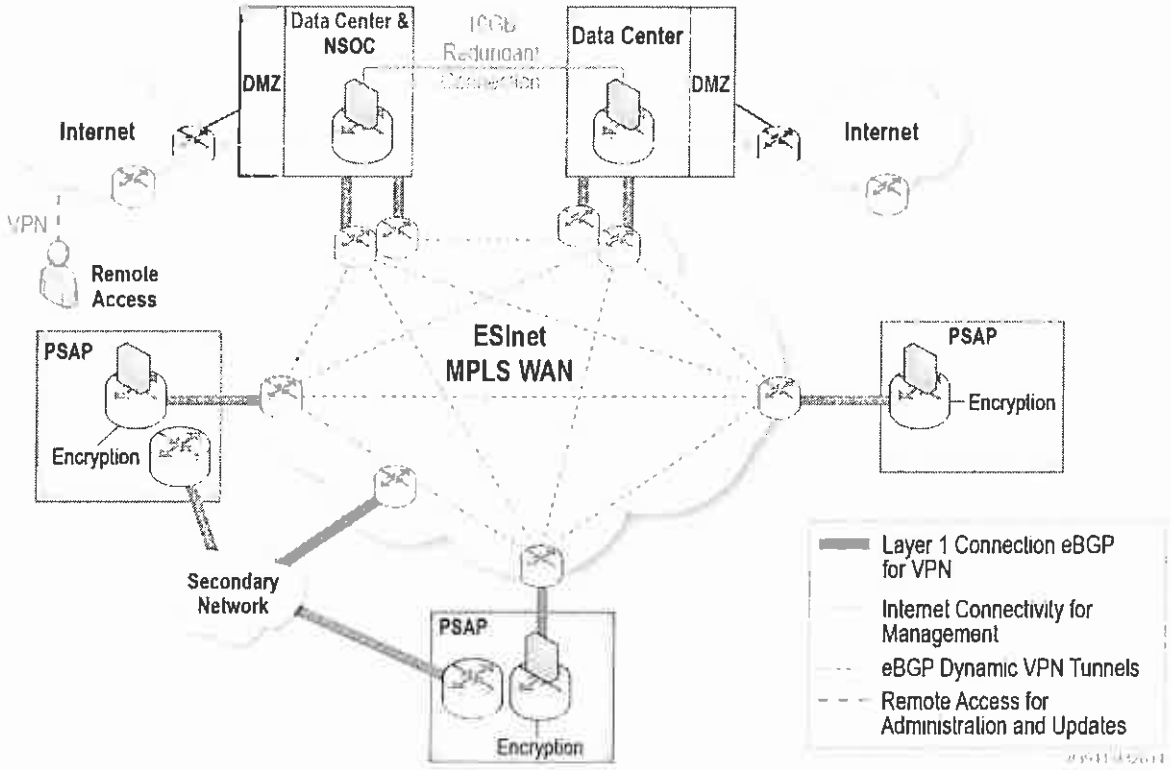


Figure 13. ESInet WAN Routing

GDIT's routing configurations, VPN architecture, and ESInet design guarantees that PSAPs will be fully functional in the unlikely event that a full data center outage occurs. The proposed design includes multiple Layer 3 open standards protocols for the Local Area Networks (LANs) and Wide Area Networks (WANs) including Border Gateway Protocol (BGP) for routing fault tolerance and Virtual Router Redundancy Protocol (VRRP) for automatic router hardware failover where dual routers exist. The solution design that GDIT is offering the Commonwealth will ensure any failed routes are automatically detected and bypassed. The IP routing design is also configured to support load balancing of calls to each of the data centers and ESInets. Although load balancing is configured within the overall solution design, the data centers and ESInets are designed, including bandwidth, to handle 100% of the Commonwealth's entire 9-1-1 call processing load.

The routing architecture proposed is vastly simplified over an MPLS mesh, supported by the predominant call flow occurring between the data center and each PSAP in a hub-and-spoke

design. Due to this hub-and-spoke design, the network routing proposed is fully scalable to support many times the amount of connections, bandwidth, and services proposed initially. Further, the provisioning of new sites or new services will have no impact on the routing for any other site.

Data Center Networking

Each data center will terminate egress traffic from the carriers as either TDM or IP. Where TDM is provided, Protocol Interface Functions (PIF) gateways will convert the traffic to IP as part of the legacy gateway implementation defined by NENA, and described in greater detail in Section 8.7, Next Generation 9-1-1 Architecture. All traffic entering the ESInet will, therefore, be IP. All IP traffic will be identified to reside in appropriate Virtual Local Area Networks (VLANs), ensuring appropriate separation of real-time and best-effort traffic, and management traffic, redundancy, and performance between routed components residing within and across multiple data centers.

The data center was designed to achieve 99.999% availability and no single point of failure. A critical design goal in achieving these requirements is to have the network design and routing operate in coordination with the NG9-1-1 applications to utilize redundancy and survivability in the means that has least impact on the operational mission. We discuss our data center design in operational 'blocks', where similar sets of tasks are isolated and behave in a prescribed manner to reduce risk, improve maintainability, and build efficiency in distributing packet processing across multiple network and application processing points. The following blocks are identified and illustrated in Figure 14:

- Data Center Core Block
- ESInet Application Block
- ESInet WAN Edge Block
- DMZ Block
- Management Block

Data Center Core Block

The data center core block is a high-speed, fully redundant LAN infrastructure that interconnects all functional blocks. It delivers high availability to support the mission-critical applications and real-time multimedia communications that drive the data center and PSAP operations, while also serving as key inspection and traffic monitoring points for network and security management. Included in the Core block is also the private backhaul connections between data centers, terminating on the Core switches.

The Core layer is based on two physically separate but logically connected Cisco Catalyst 4500x switches, which provide high availability without increasing routing complexity, improving overall usable network bandwidth and resiliency, and simplifying maintenance. The Core block provides layered security enforcing deterministic traffic flow patterns, where traffic undergoes critical inspection and policy management.

To meet and exceed the mission-critical requirements of the redundant Catalyst 4500x switches, each switch will utilize Virtual Switching Systems (VSS), providing the following benefits:

- Delivers simplified network operations by:

- Providing a single point of management, allowing updates, policy changes, and configurations to be synchronized between the two switches.
- Forming Multi-chassis Etherchannel (MEC) to the logical switch that provides a loop-free topology and eliminates the need for spanning tree protocol.

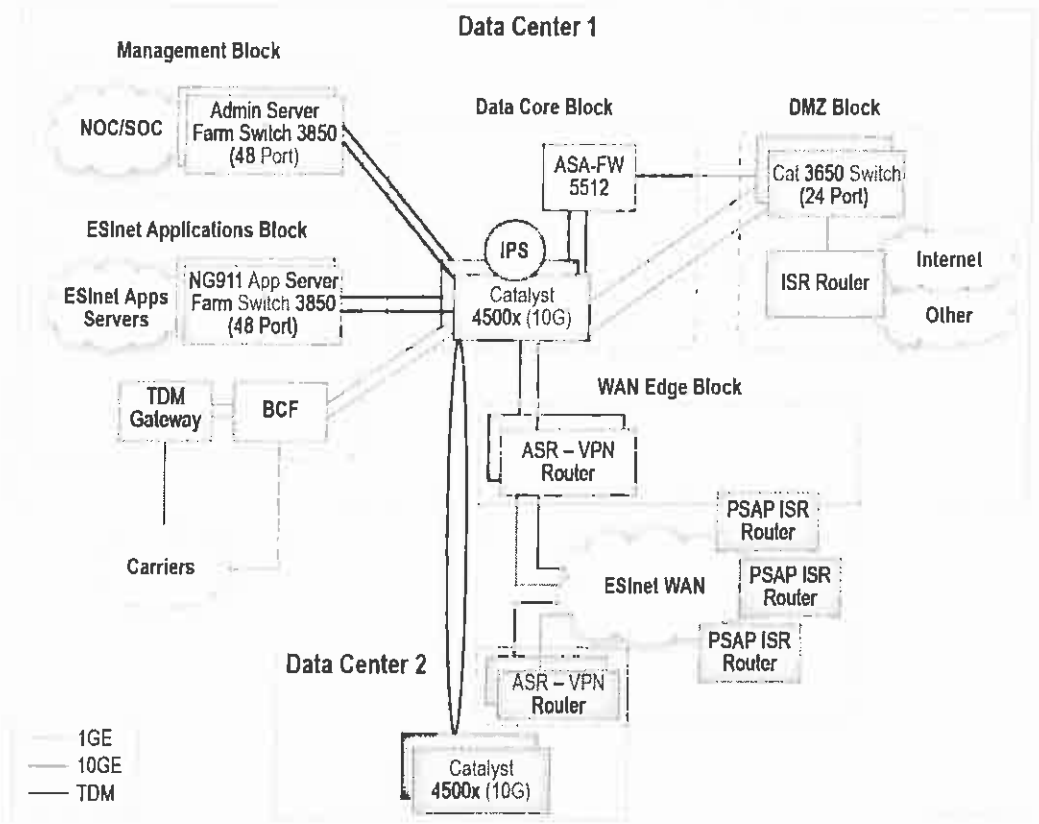


Figure 14. Data Center Networking

- Eliminating complexities of managing, tuning, and troubleshooting first hop routing protocols like Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP).

- Improves resiliency through:
  - Providing stateful failover between the supervisors on the two chassis. Provides sub-second failover and transparent failover even to delay sensitive applications like voice and video.
  - Extending Etherchannels across two physical chassis provides for increased resiliency using MEC to minimize traffic disruption from switch or uplink failure.
- The active-active MEC extended across two physical chassis improves bandwidth utilization.

ESInet Application Block

The ESInet application block is where all ESInet applications reside and communicate through the Cisco Catalyst 3650 switches in a stacked configuration. Each of the ESInet applications within the data center is deployed in an high-availability architecture, and it is redundant across multiple data centers to ensure 99.999% availability.

ESInet WAN Edge Block

The WAN edge block provides routing across the ESInet WAN between data centers and all PSAPs, remote locations (NOC/SOC, training, etc.) and other data centers. The selected Aggregation Services Router (ASR) (at the data center) and Integrated Services Router (ISR) (at a PSAP) will terminate GRE tunnels from each location, apply and manage QoS tags to the MPLS packets, and apply route filter to ensure the BGP route tables are secured. Additional critical functions of the edge routers include:

- Serves as a demarcation point to the ESInet WAN, where SLAs with the WAN provider will be managed to ensure end-to-end service performance.
- Serves as the Policy Enforcement Point (PEP) for monitoring and management of security, providing stateful firewall, intrusion detection, and encryption.
- Provides a critical monitoring point for QoS and network management through the flow of management traffic, including netflow, SNMP, WMI, IPMI, ICMP, SSH, and SYSLOG.

DMZ

The DMZ block was designed to isolate all ESInet access that is not entering or leaving the data center through the ESInet WAN or BCF, providing additional levels of security, inspection, and authorization. DMZ will provide the services necessary, including stateful firewall, intrusion detection, and packet inspection of all traffic, and create a security landing zone for remote client VPNs.

Management Block

The management block provides the flow of management and administrative traffic critical for network and security operations. For increased security, management traffic will segregated by VLAN where possible to disassociated media from managements.

Remote Site Networking

The PSAP routers will utilize 26xx and 34xx series ISR routers, with the selection of specific models based entirely on bandwidth throughput requirements. PSAP routers provide the critical routing connections between each PSAP and each data center, and serve as the critical policy enforcement point for all security, QoS, and management across all available network connections. Routing will be established utilizing multiple Layer 3 VPN tunnels between each PSAP and each data center using Dynamic Multipoint VPN functions, outlined in Figure 14. Additional benefits of the VPN architecture include:

- Redundant GRE/IPsec tunnels are provided in an active-active state, to ensure the timeliest failover times are obtained, and to ensure the backup path is operational when needed.
- Provides MPLS and BGP functionality at each PSAP.

- Supports the use of multiple carrier connections for secondary or tertiary network redundancy, including separate MPLS Customer Edge (CE) instances where carriers require isolated routed loops.
- Reduced routing complexity of an MPLS mesh, simplifying management and maintenance.
  - Provides separation of distinct traffic types allowing for improved management of QoS and awareness of network availability.
  - Each PSAP router will be configured with the advanced security bundle, providing stateful firewall and Intrusion Detection (IDS). The firewall functional will ensure all packets destined for the PSAP are being sent and received from expected sources. IDS is a deep-packet, inspection-based solution that stops malicious traffic at the PSAP, where virus and threats are most likely due to user activity.
- Demarcation point between the ESInet WAN and the PSAP such that SLAs can be managed across the ESInet WAN.

The PSAP edge switches will utilize the Cisco Catalyst 3650 to establish the QoS policies and apply traffic marking by policy, including voice, video, data, and management. The edge router will inspect these QoS attributes to ensure traffic policies are intact and reapply QoS attributes as necessary. The edge router will also police the WAN links for QoS and allow WAN throttling to enforce and ensure policies. All switch ports, both used and unused, will be monitored by the Terminal Access Controller Access-Control System (TACACS) for changes in state to enhance security. Additional features of the Catalyst switch include:

- Power over Ethernet (PoE) on all ports
- Stackable
- Provides logging and monitoring capability
- 802.1x authentication for managed devices and users, web authentication for guests or non-802.1x users, and MAC authentication bypass for unmanaged or non-802.1x devices
- Prevents MAC address-flooding attacks by limiting the MAC addresses of stations allowed access to the same physical port

All PSAP routes have been selected to support scalability and growth, to support growth n call volume, positions, and/or payload enhancements. Scalability considerations include:

- All routers provide at least 200% of required bandwidth throughput to support growth in positions and service payload.
- The PSAP router and switches have additional ports to support additional workstations, printers, recorders, voice appliances and other required devices.
- Redundant switches are configured to be stacked to allow the addition of ports, bandwidth, or resiliency through the incremental additional of another switch (if required).

All PSAP routers have the Cisco survivable voice gateway feature and analog (FXS/FXO) interfaces directly on the router to support administrative calling utilizing local PSTN trunks and lines. Under typical operation, the control of these calls will be managed by the Cisco

CallManager located at each data center. Should the PSAP become isolated from the data centers, the local voice gateway provided in the routers will provide call control to receive and make PSTN calls. Further information is provided in Section 8.7.26 (Administrative Lines) of our proposal. Limited secondary PSAP routers will utilize 19xx series routers without the voice gateway functionality, as described in detail in Section 8.7.31, Limited Secondary PSAP Equipment.

PSAP routers will provide management of available network connections, including primary, secondary, and tertiary, where available. Where redundant connections are provided, redundant routers will be provided to ensure availability and redundancy, with each router capable of supporting 100% of the local service requirements. Redundant routers will share a default gateway address to enable seamless failover should a system failure occur. GDIT's proposed solution has identified four basic PSAP configurations, representing variation in bandwidth throughput and the addition of multiple routers for redundancy. General (non-site-specific) comments on each model are provided with Figure 15 through Figure 18.

Large PSAPs will utilize a fully redundant configuration with high-availability primary and secondary connections utilizing MetroEthernet connections across multiple carriers, optional tertiary connections, and termination of local PSTN trunks.

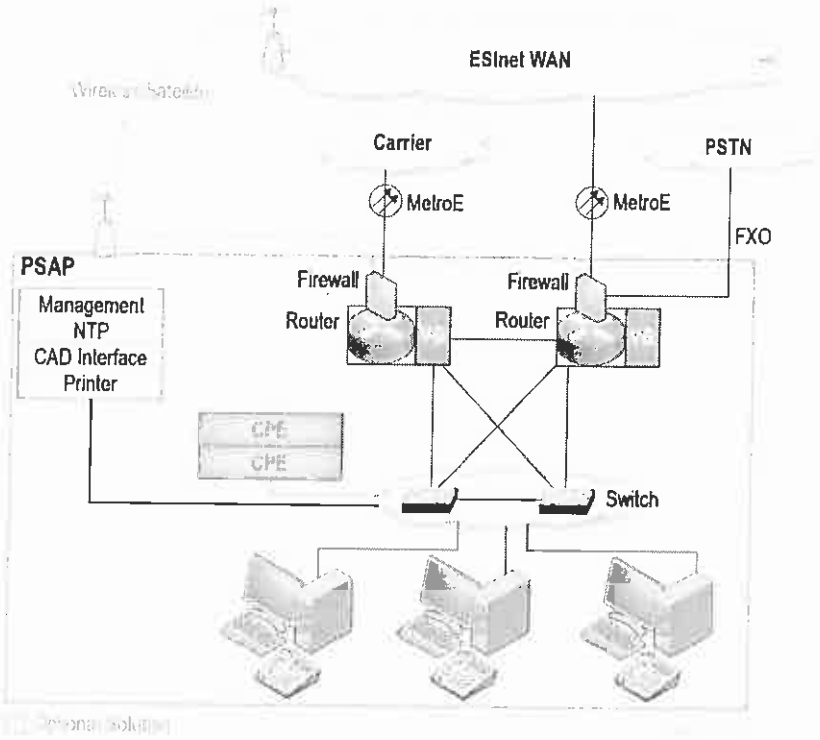


Figure 15. Large Model PSAP (17–45 Positions)

Figure 16 represents two PSAP models reflecting an identical fully redundant configuration and differing only in the bandwidth throughput of the selected routers.

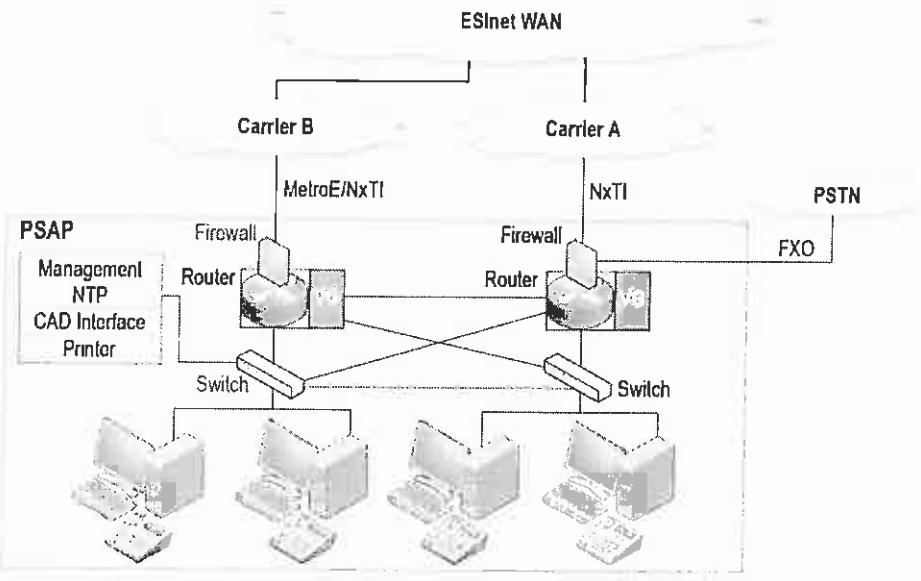


Figure 16. Medium (9–14 Positions) and Small-Medium (6–8 Positions) PSAP

Small PSAPs are deployed with the optional addition of redundancy, including redundant network connection and associated redundant routing. Redundancy can be added incrementally without impact on live operations.

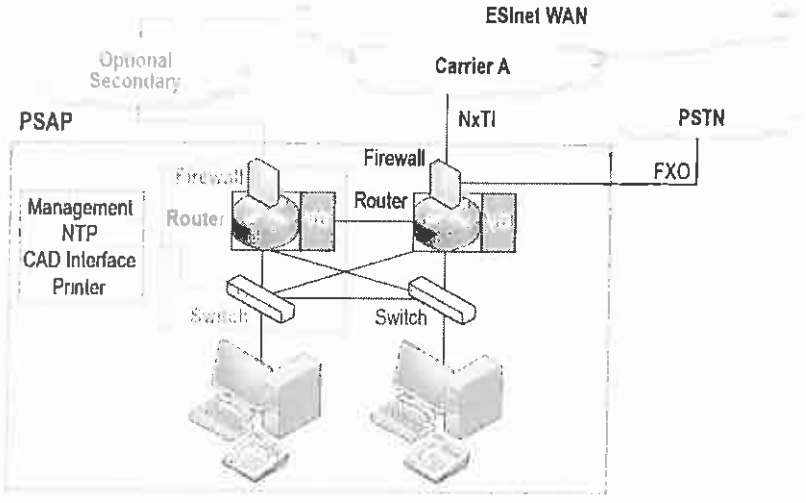


Figure 17. Small PSAP (2–5 Positions)

Limited Secondary PSAPs will utilize the Cisco 19xx series ISR router to provide connectivity to the ESInet utilizing a T1 interface. The 19xx series router has all the same QoS and security capabilities of the 26xx series router, but does not support the voice gateway feature.

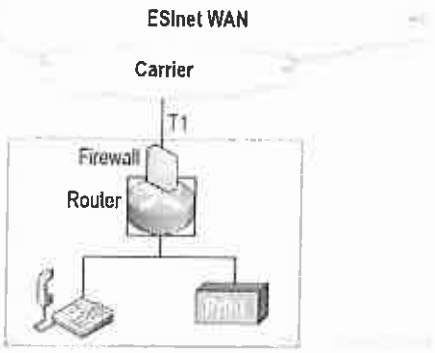


Figure 18. LImited Secondary PSAP

Quality of Service

All networking of NG9-1-1 traffic is performed with the fundamental requirement of achieving 'carrier-class' QoS. While not all traffic in the solution is voice, voice does have the strictest requirements, and it is safe to assume that achieving good voice QoS provides by extension good overall service QoS. The primary measure of voice QoS uses Mean Opinion Score (MOS), and a score of 4.0 or greater is typically considered carrier grade. GDIT's proposed solution will provide an average MOS score of 4.0 or greater.

MOS is a traditional measure of voice quality that emanates from a human hearing assessment. Today, MOS is measured using one of two techniques: in a calculated method, systems report on the transit performance of packets (packet loss, jitter and delay) at intervals, and these measures are used in a calculation of MOS. This method does not consider several factors that are not measured by packet performance, including echo and volume. Further, the interval measurements are typically average measurements over the duration of a call that do not necessarily reflect any instantaneous problems, such as choppy voice.

By far, the most accurate and meaningful method for determining MOS (short of human hearing) is to capture and measure the actual media stream. GDIT's proposed solution allows for both methods, utilizing information from systems to continuously report on key performance indicators like MOS and packet performance. Furthermore, our proposed solution deploys the Oracle Palladion monitoring system, with probes placed at each PSAP and data center to capture and measure actual media as it ingress and egresses the network.

The 'hosted' NG9-1-1 model proposed by NENA leverages an IP converged services approach, where services of differing types are delivered to remote locations over a shared use infrastructure. Where meeting the performance requirements is fundamental, GDIT also leverages our extensive experience to build a deterministic environment, where service quality is assured based on predicated relationships, actions, and controls. We identify three primary considerations for achieving systemic, end-to-end performance with deterministic QoS:

- Bandwidth
- Traffic Engineering
- Network and Security Monitoring

Bandwidth

GDIT has provided detailed understanding of minimum bandwidth requirements based on worst-case, simultaneous use, aggregate service demands, supporting all existing payload types and most (anticipated) future payload types. At the same time, GDIT notes that bandwidth has a high recurring cost and is relatively simple to add incrementally as long as spare termination capacity is planned.

Bandwidth availability is a critical consideration in achieving QoS, ensuring that sufficient network resources exist to carry all services. Our solution has engineered the bandwidth to support a worst-case scenario of 100% active PSAP positions across the Commonwealth with dual calls per PSAP. GDIT has also engineered the bandwidth as well as provided the expandability and scalability for future PSAP position growth and new NG9-1-1 payload types.

As identified in Section 8.3.3.1 (ESInet Demarcation Point), GDIT's proposed solution utilizes a minimum total bandwidth per call taker position of 500K, and we have included in our solution the recommended bandwidth of 750k per call taker position.

Traffic Engineering

Where bandwidth offers the necessary pipe for services, instantaneous demand for bandwidth, 'bursty' traffic demands, and packet size can often cause congestion at routing points, (somewhat) independent of available bandwidth. Best-effort services, such as file transfer and web traffic, tolerate packet sequencing problems using buffers and/or resending 'lost' packets. Real-time services, however, cannot tolerate such sequencing problems, and each 'lost' or out-of-sequence packet serves to degrade the media. Traffic engineering provides a set of prioritization mechanisms, including Type of Service (ToS) and Diffserv, which allow 'marked' packets to enable sequencing of high-sensitivity traffic over that of lower-sensitivity traffic to achieve best QoS for all services.

Common networking requirements that support end-to-end real-time services include:

- Real-time traffic should comprise no more than 50% of total available bandwidth.
- Real-time voice traffic should be configured L3 tags leveraging TOS and Diffserv as follows:
  - (L3) DSCP Voice = EF46
  - (L3) DSCP Video with Audio = EF45
  - (L3) DSCP Interactive Video = AF41
  - (L3) DSCP Streaming = 32

The Commonwealth has defined packet performance criteria as packet loss (0.5%), jitter (20ms), and (round trip) delay (20ms). GDIT has based our networking design and connectivity on achieving this performance, and our solution complies with this requirement. Our assessment is that this requirement is very strict, and that industry best practices for end-to-end real-time services for packet loss, jitter, and (round trip) delay are 2%, 20ms, and 80ms, respectively. While the increased performance does provide a buffer to degraded conditions, it offers little increased QoS and imparts significant complexity and cost in achieving and managing network provider SLAs.

Network and Security Monitoring

Traditional E9-1-1 (TDM) services are 'deterministic' where service is (largely) either working or not, subject to 'hard' failures that are highly apparent, and allowing for reactive maintenance. Rarely in the traditional environment will services be working but of marginal quality.

The IP services model has the additional burden involving a wide range of 'soft' conditions that are both transient in nature and granular in severity. In large part, these conditions are the result of contention for shared resources across the entire IP services domain. The various techniques provide an excellent approximation to a deterministic environment. However, the only means for validating service quality, particularly for real-time services of voice and video, is through real-time monitoring of every session. Such monitoring can determine hard failures for reactive maintenance, but equally important, it can provide critical trending analysis of Key Performance Indicators (KPIs) that allows proactive maintenance to prevent future problems. Monitoring for proactive maintenance is, therefore, a key component of the service assurance model.

8.3.2.1. PSAP Network Bandwidth

Bidders shall complete Attachment F- PSAP Network Bandwidth and shall describe in detail the bandwidth requirements for the system. The contractor shall verify that the proposed bandwidth is adequate to handle anticipated traffic based on the contractor's independent calculations The contractor shall also provide predicted future bandwidth requirements.

GDIT will comply with the RFR requirements.

The minimum required bandwidth per call taker position is identified as 500 kbps. The recommended bandwidth per call taker position is 750k. These calculations are defined as follows, and they included in the PSAP Network Bandwidth in Attachment F.

- 110k per voice call times two (2) active calls per PSAP position, to include Short Message Service (SMS, or texting) = 220k
- 20k per position for call control and management traffic
- 256k per position to support NG9-1-1 GIS mapping

The minimum bandwidth required, therefore, assuming absolutely no statistical averaging of call taker activity and 100% demand from all positions simultaneously is 500k per call taker position. GDIT recognizes, however, that increased demands will be placed on the network in the future, including potential growth in the number of call taker positions, increased image/mapping resolution, and new payload types. The following provides a brief of our expectations for new payload bandwidth demands:

- **Multimedia Messaging Service (MMS)**: MMS includes the transmission of (typically) low-resolution still and video images in conjunction with text. MMS is not (typically) real-time traffic and is tolerant to best-effort service, placing minimal demand on bandwidth requirements. An additional 20k should be sufficient for MMS.
- **Documents**: Document transfer will typically be delivered from the Call Information Database (CIDB) and may include a wide variety of formats. It is expected that NENA document standards will seek to eliminate the use of very high resolution to minimize storage and transport bandwidth. Similarly, the transfer of these files is not real-time and

will tolerate best-effort services. GDIT assumes a 30k incremental demand for document transfer.

- **Video**: By far, video can present the most demanding of additional bandwidth payloads, with high variability on the types of video payloads, control protocols, and required resolution. Some video is also real-time in nature, causing additional network intensity. NENA standards are still considering all video options. GDIT expects that 256k of additional bandwidth will serve many initial requirements, but that support for increased resolution, new payload types, and increased frequency of video will place additional demands on the network in the future. GDIT's proposed solution is scalable to support increased demands beyond the initial implementation.

To support considerable future demands, GDIT has included in our proposed solution an additional 250k of bandwidth per position. As such, GDIT's proposed solution has utilized 750k per PSAP position when determining all WAN bandwidth and connectivity requirements. We believe that this consideration will serve the Commonwealth well into the future. Furthermore, when considering statistical network utilization, 750k per PSAP position may fully support the end-state requirements, eliminating the need for wholesale circuit upgrades.

GDIT notes that larger sites utilizing access loop fiber connection to the ESInet WAN Core are oversubscribed as compared to the recommended bandwidth calculations. These connections offer the defined throughput as a best-value approach in supporting expected future services. Aggregation of all traffic across the data center connections maintains a 750k per call taker position calculation.

Limited Secondary PSAPs do not deploy call taker workstations, but rather allow conferencing (transferring) of calls from a primary PSAP to a local IP phone with display of location information (on the phone) and printing of location information to a local network printer. Limited Secondary PSAPs will be connected to the ESInet utilizing a Cisco edge router, and they will be subject to identified traffic engineering for QoS, requiring 256k of bandwidth. GDIT has proposed primary connections to all Limited Secondary PSAPs utilizing T1 access loops from (primarily) Verizon as the minimum available (compliant) solution. As T1s provide a 1.5 MB of bandwidth, GDIT believes that Limited Secondary PSAPs are an excellent candidate for using only the secondary connections of MBI and/or public Internet as a best-value solution.

8.3.3. Diverse Network Entries

The State 911 Department training centers and certain regional PSAPs and RECCs, as determined by the State 911 Department, shall have physically redundant entrance facilities so that there will be no single points of failure in the network. Therefore, the network shall include physically diverse building entrances for certain PSAPs, to be identified by the State 911 Department. In certain cases, where it is not feasible to connect a PSAP by diverse wireline links, the PSAP may be connected with microwave or satellite or wireless links, in order to provide these redundant connections. To the extent that dual entrances are required, the switch between diverse network connections shall be automatic and seamless to PSAP operations.

GDIT will comply with the RFR requirements.

GDIT's proposed solution is designed to ensure 99.999% availability with full redundancy of systems. Network connections will be redundant for all PSAPs with greater than five (5) positions, and all smaller PSAPs will support redundancy as an option. As described in Sections 8.3 (ESInet) and 8.3.1 (Network Design), both fixed wireless (microwave) and satellite have

been provided in our solution. Fixed wireless will offer significant cost and performance benefits to the Commonwealth, although only select sites will have availability to this technology. Upgrades based on the Commonwealth's request can be discussed. Satellite coverage is offered to all sites as a tertiary option. Based on Q&A responses from the Commonwealth, it is understood that the following 9-1-1 facilities currently have physical and redundant entrance facilities:

- Boston Police
- Cambridge Communications
- Essex County Wireless Center
- Essex County Regional Emergency Communication Center (RECC)
- Framingham State Police
- Maynard TC CS100
- Maynard TC Pallas
- Newton Police
- Springfield Communications

The PSAP ISR routers providing the network edge to the ESInet will terminate all network connections, including primary, secondary, and tertiary. Each ISR router implements IP-SLA routing features, which will select the best network based on established policies, including response times, packet performance, cost, and time of day.

8.3.3.1. ESInet Demarcation Point

The network connection shall be located in the same room as the Next Generation 911 system (which shall be in the same room as the 911 backboard), unless otherwise directed by the State 911 Department. The contractor shall provide the necessary connection at the network demarcation point and all required hardware (cabling and electronic components) to connect the network to the Next Generation 911 system.

GDIT will comply with the RFR requirements.

GDIT provides a turn-key solution of NG9-1-1 systems and services to enable a high-availability and NENA-compliant NG9-1-1 migration from the E9-1-1 environment. GDIT will provide all network connections. As part of our migration plan, every site will be evaluated for physical characteristics pertaining to installation of systems and enablement of new services, including power, cabling, and space. All NG9-1-1 ESInet systems will be placed in the same location as the network demarcation and 9-1-1 backboard unless directed otherwise by the State 911 Department, and the systems will include all required cabling and systems to ensure functional requirements. Our team will be coordinated by a dedicated Project Manager, who will provide on-site discussions with local managers to ensure an implementation and migration plan that best meets the operational needs of the site, complies with RFR requirements, and provides customization of the physical infrastructure where possible. Prior to migration, the site implementation plan, design, and schedule will be communicated to local managers for comment and review.

8.3.3.2. Network Failover

The system shall have a network failover scheme that is widely used in the industry and that complies with open standards and that provides for maximum availability. availability. Bidders shall describe in detail the proposed network failover scheme that provides instant switchover from failed or degraded components, systems, networks, and data centers. The system shall meet a 99.999% standard of availability. There shall be redundant, dual Ethernet

switches (and, if required, routers) at PSAPs to be identified by the State 911 Department and, if required, equipment to accommodate diverse communication service providers at PSAPs to be identified by the State 911 Department. The contractor shall assess the use of technologies such as WAN Virtualization, microwave, satellite, and wireless technology to improve ESInet resiliency, redundancy, and availability, and shall include the assessment in the network design document.

GDIT will comply with the RFR requirements.

GDIT's proposed solution is designed to meet 99.999% availability while ensuring the call quality meets the Commonwealth's MOS 4 and above performance standards. GDIT's proposed architecture provides component-level redundancy, as well as an overall resilient network design architecture.

As stated by the requirement, "redundant dual Ethernet switches and routers will be deployed and configured at PSAPs to be identified by the State 911 Department and, if required, equipment to accommodate diverse communication service providers at the State 911 Department identified PSAPs." The Q&A responses received from the Commonwealth stated that after award the locations requiring dual switches and routers would be determined.

GDIT has identified PSAP network models utilizing selected Cisco ISR routers, as illustrated in Section 8.3.2, System Networking Requirements. With very few exceptions, all models provide exactly the same functionality and routing of services, with the only difference being the throughput bandwidth supported by the router and the use of single or redundant routers. In all cases, where a single router is used, an optional second router can be placed to support site redundancy requirements. In this manner, each site is deployed in exactly the same configuration, with exactly the same routing capabilities and policies.

All redundant networking devices will be deployed in a stacked configuration or using a first hop routing protocol like Virtual Router Redundancy Protocol (VRRP). Stacking offers the advantage of allow IP configuration simplicity and modularity, but is otherwise equal in offering failover redundancy to VRRP.

As previously noted, the edge router will utilize IP-SLA policy routing to identify best and/or preferred network paths where multiple networks exist. This will ensure proactive switching to ensure network redundancy and failover.

8.3.4. Network Performance and Service Levels

The contractor shall ensure that network services meet the following minimum requirements:

- *The network services shall be deployed using a highly reliable architecture with reliability, availability, and survivability incorporated into the design wherever feasible.*
- *The network services shall be designed to automatically reroute all data types around broken or failed links without manual intervention.*
- *The network services shall be capable of prioritizing critical traffic over other traffic by user, by application, by time of day, date, or a combination of criteria. The network shall support multiple levels of prioritization to ensure that the most important applications or users have the access and bandwidth that are required for successful communication.*
- *The network services shall be capable of treating content through prioritization and bandwidth management to provide guaranteed Quality of Service (QoS). In the event of a disaster, where security and public safety applications shall have priority, the network shall automatically adjust QoS for prioritization. The network shall maintain a toll quality of MOS 4.0 or better.*

- *The network services shall use traffic shaping and traffic policing to ensure that the network meets or exceeds its performance contract requirements.*
- *The network services shall operate on a 24 x 7 basis.*
- *The contractor shall, within sixty (60) days following contract award, submit to the State 911 Department for approval a chart or list of "Outage Escalation Procedures" that shall be adhered to*

GDIT will comply with the RFR specification.

GDIT has proposed a purpose-built NG9-1-1 network to meet the performance and availability requirements identified by the Commonwealth. Our solution provides four primary categories of redundancy and failover:

- **Applications** – Each application in the NG9-1-1 environment that is used in performing tasks related to NG9-1-1 routing or services is deployed in a high-availability (HA) model within each data center. Most application will use a VRRP method to failover between individual systems, should one encounter a problem. In this manner, each data center supports 99.999% availability for applications. The use of multiple data centers further enhances the reliability model by enabling an active-active or active-standby model between data centers for each application. With this, application failure is redundant both within a data center and across multiple data centers.

- **Networking** – The data networking design provides a purpose-built unified communications infrastructure leveraging NENA standards, the exceptional experience of the GDIT team, and widely accepted best practices for delivering converged services over a shared infrastructure. Both inter-site (LAN) and intra-site (WAN) routing is designed to be fully redundant to support multiple interfaces and service-aware capabilities for failover. Routing across the network is highly secure, leveraging encryption and VPN tunnels, and the QoS is highly deterministic, leveraging bandwidth analysis and traffic engineering.

- **Telecommunication Circuits** – GDIT and our partner Windstream have collaborated to deliver the Commonwealth a composite set of connectivity services that meets the performance requirements of services transport and offers exceptional flexibility for leveraging diverse carriers, technologies, and network facilities. The Windstream high-speed Core provides a highly available and redundant solution with proven SLA management. Further, the Windstream numerous NNI (aggregation points) maximizes the ability for the Commonwealth to use other private or leased facilities/networks and interconnect to the Core seamlessly.

- **Management** – All redundancy and availability are supported by a holistic approach to network management where services are monitored on a 24x7x365 basis for KPIs, and enabling proactive and reactive maintenance to occur in response to hard and soft failures. Continuous monitoring is supported by the Needham, Massachusetts Network and Security Operations Center (NSOC) and Help Desk operating 24x7x365 to provide around-the-clock support. GDIT also provides backup centers of excellence with additional subject matter experts in security operations, located in Herndon, Virginia and in sustainment operations, located in Fairview Heights, Illinois. All aspects of performance will be tracked and reported to the Commonwealth, with attention to QoS and compliance to KPIs.

GDIT will have comprehensive awareness of services quality, systems health, and compliance with required KPIs across all available network connections, ensuring that prioritization and QoS is managed regardless of network selection. We leverage over 20 years of experience in providing sustainment to mission-critical networks to ensure all contingency plans and communication paths are established. Within sixty days of award, GDIT will detail our Outage Escalation Procedures and submit them to the Commonwealth for their review.

8.3.4. Service Level Agreements

The contractor shall ensure that all network service providers shall execute a service level agreement ("SLA") that shall, at a minimum, address the following:

- *Network performance level and QoS requirements;*
- *Response requirements to various types of service disruptions;*
- *Response times and requirements for new installation or changes;*
- *Network management, monitoring and reporting times and requirements; and*
- *Penalties and other consequences for non-compliance.*

The contractor shall submit to the State 911 Department all SLA(s) executed with network service providers within thirty (30) days following execution of such SLA(s), and shall promptly notify the State 911 Department of any and all changes in network service provider.

The SLA(s) shall include the following requirements, at a minimum:

GDIT will comply with the RFR specification.

Each edge router will perform traffic engineering, traffic monitoring, and packet inspection as a means of identifying end-to-end performance of services, with the monitoring systems delivering reports on KPIs. Reactive maintenance will be initiated by the NSOC or autonomously by the network or the applications to ensure survivability of alternate systems or paths. Proactive maintenance will seek to identify soft failures and where compliance to KPI and SLA will occur.

Our transport partner, Windstream, has excellent experience in providing exceptionally high transport performance within their Core network, and we are confident that their Core will meet or exceed the specified requirements. Similarly, Windstream has worked in conjunction with most primary carriers to understand the expected quality of their network, how their networks connect to the Windstream Core, and how resolution to KPIs is achieved. This includes work with Verizon, Level 3, and Axia.

Following award, GDIT will further discuss with selected access loop providers to ensure SLA requirements are met and delivered. SLAs with every service provider will be monitored on a continual (24x7) basis and will include packet performance and QoS, response times to network conditions based on severity levels, response times for new or changed services, and reporting. GDIT will document and submit all SLA agreements following execution, or any subsequent change, to the Commonwealth within 30 days of agreement. A direct and continuous path of communication will be established with each provider to ensure immediate response to issues and understanding of our shared performance requirements. GDIT will report to the Commonwealth all performance metrics and initiative any necessary corrective action.

8.3.4.1. Packet Latency (20 ms)

Packet Latency to an average round trip time of forty (40) milliseconds which equates to a one (1) way transmission time of twenty (20) milliseconds. Packet Latency is measured between the demarcation points, typically between a

data center demarcation point and a PSAP demarcation point. Bidders shall identify the packet latency for proposed tertiary networks (the MOS for any such proposed tertiary networks shall be a minimum of three (3)).

GDIT will comply with the RFR specification.

GDIT will meet total packet latency requirement of 20ms for all primary and secondary path connections, including for fixed wireless connections and will support a MOS of 4.0 or greater. End-to-end latency for satellite connections will be less than 720ms. Satellite will support MOS scores of 3.0 or greater.

8.3.4.2. Packet Loss (0.5%)

Monthly average packet loss between demarcation points not to exceed 0.5%.

GDIT will comply with the RFR specification.

GDIT will meet the packet loss performance requirement of 0.5% for all primary, secondary, and tertiary path connections. End-to-end packet loss of less than 0.5% is supported by the proposed satellite technologies.

8.3.4.3. Jitter (20 ms)

Jitter shall not exceed twenty (20) milliseconds.

GDIT will comply with the RFR specification.

GDIT will meet total jitter performance requirement of 20ms for all primary and secondary path connections. The satellite alternative will meet <40ms of total jitter.

8.3.5. Performance Degradation and Circuit Failures

The contractor shall monitor network performance and shall track, identify, document, and report to the State 911 Department the following failures in circuit performance: two (2) or more identical or similar circuit failures or performance degradations within thirty (30) calendar days; and five (5) or more dissimilar circuit failures or performance degradations within thirty (30) calendar days. For all such failures, the contractor shall submit a remediation plan to the State 911 Department for approval.

GDIT will comply with the RFR specification.

GDIT solution will include the regular release of performance reports on end-to-end services and KPI. Included in our web-based reporting will be access to reports on trouble tickets opened, aging of tickets, and severity of tickets. An action register will be maintained, with all responsible partners and parties for tracking and regular reporting to the Commonwealth. Please refer to details on GDIT's NSOC and Help Desk in Section 8.20, Warranty, Maintenance, and Monitoring.

8.3.6. Timely Installation Intervals for New Service Requests

The contractor shall complete new service installation within sixty (60) days of a request.

GDIT will comply with the RFR specification.

GDIT has evaluated available access loops from each PSAP to the Windstream Core from multiple carriers for price, availability, and performance (to RFR requirements). In all T1 provided sites, circuits are in place and can meet a sixty (60) day availability from date of

request. Windstream has consistently met this installation parameter as part of its ITT09/ITT46 contract for copper facilities.

Optical circuits provided from the Windstream Core and by third-party providers are expected to be available within sixty (60) days of request, although some routes may need to be negotiated upon order due to construction-related requirements. The GDIT team will fully manage the availability for any potential problem areas and report the status to the Commonwealth

8.4. NETWORK SECURITY

Our collaborative approach for the MA NG9-1-1 system security harnesses innovation, hardened processes, synergies, and expertise across our company's longstanding history of delivering security solutions for our customers. Our objective is to become an integral partner of the Commonwealth and to help the Commonwealth achieve their security goals and assist in delivering a secure, integral network environment.

GDIT understands the security requirements as prescribed by the RFR. We have proposed a security solution that satisfies all security requirements and have verified our solution against the NENA 75-001 Security Guideline and the Criminal Justice Information Services (CJIS) Security Policy for compliance. Additionally, all MA NG9-1-1 security requirements were satisfied against the backdrop of supplemental industry standards and guidelines, such as National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), which we commonly use to deliver security solutions for similar environments. GDIT maintains an experienced team of security architects, cyber-analysts, and administrators that can establish and maintain cybersecurity operations through best practice approaches prescribed by NIST, the Defense Information Systems Agency (DISA), and FISMA.

8.4.1. General

In addition to all other requirements set forth herein, the contractor shall comply with current FBI Criminal Justice Information Services (CJIS) Security Policies as set forth on http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view, shall comply with such FBI Criminal Justice Information Services (CJIS) Security Policies as may be issued in the future, and shall apply a variety of security measures to ensure that:

- *Network operations are not disrupted;*
- *Unauthorized individuals do not gain access to the network;*
- *Least access policy is applied;*
- *Data theft does not occur;*
- *Monthly vulnerability scans and assessments occur;*
- *Incidents are logged, reported, and responded to;*
- *Changes are logged and managed;*
- *Activity, incidents, events, and changes are maintained to support routine and forensic audits;*
- *Data is not modified or deleted;*
- *Intrusion protection/Intrusion detection is implemented; and*
- *Identity theft does not occur.*

These measures shall include physical safeguards, operating system hardening, hardware and software information security best practices, stringent change management processes, security incident response, resources, educational efforts, and organizational policies.

The contractor shall provide all necessary appliances, including firewalls, routers, switches, intrusion protection/detection, and cabling to ensure network security for each PSAP and data center.

The security architecture shall withstand sophisticated attacks, including without limitation, distributed denial of service attacks, while maintaining system functionality. Bidders shall describe in detail how the system shall withstand such attacks.

GDIT's proposed security architecture fully complies with and supports the RFR requirements, and it will also fully comply with Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) security policies as we operate and maintain the NG9-1-1 network. GDIT delivers a holistic security capability that leverages a defense-in-depth approach, where traffic is forced to visible and known points of entry, eliminating uncontrolled avenues of attack and enabling defensive controls, monitoring, and threat remediation. Defensive controls are policy-based traffic mechanisms, such as traffic separation, blocks, redirects, and encryption, which are placed at the network transport boundary to manage and restrict the flow of traffic. Monitoring is the real-time capture of systems-generated "management" information, such as packet performance, log reports, and user activity reports, which provide critical visibility into the flow of information across the network. Remediation provides for understanding of where and how attacks are occurring or have occurred such that the exposure of information can be assessed and new mechanisms and policies can be built to prevent future exposure.

Figure 19 illustrates GDIT's defense-in-depth security approach, highlighting the use of controls, monitoring, and remediation, and the collection of critical management information. Also illustrated is the centralized definition of policies that define the permissions and rules for the defense-in-depth approach, from the user level to the service level and the packet level.

The MA NG9-1-1 security architecture will be designed to maintain network operations and the core emergency health and public safety service that the Commonwealth will demand of it. Mission assurance and integrity are the cornerstones for every service-oriented network infrastructure. With that understanding, GDIT, through proper design approaches, process, staffing, and tools will ensure the following:

- Network operations are sustained with minimal downtime, with the mission objective to ensure that network operations are not disrupted.
- Unauthorized individuals or parties do gain access to the MA NG9-1-1 network.
- The appropriate network and physical access policies and procedures are applied.
- Routine monthly vulnerability scans and assessments occur and are managed through the Vulnerability Management System and supporting policies.

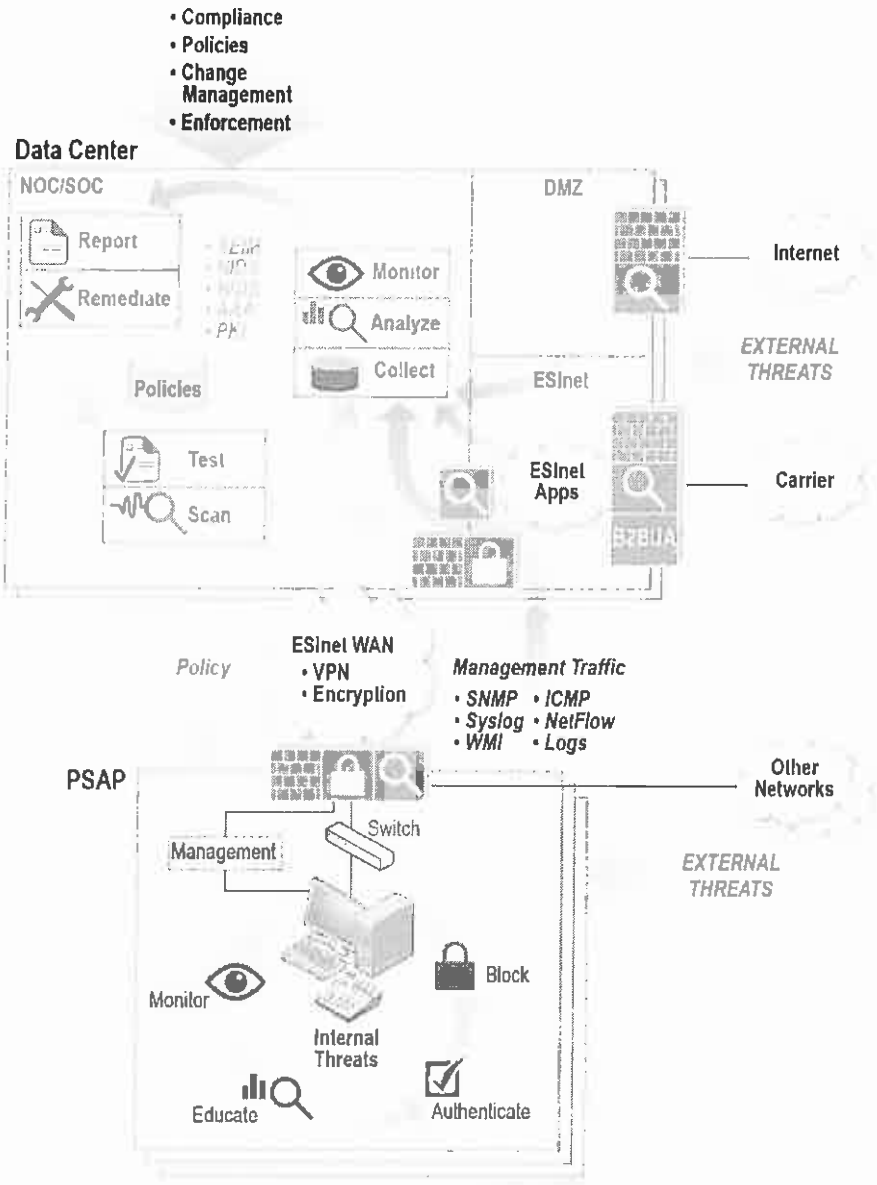


Figure 19. GDIT's Defense-in-Depth Security Approach

- All security incidents are logged, reported, and remediated with the appropriate workflow and incident prioritization applied.
- MA NG9-1-1 changes are documented and managed appropriately.
- Security events and reported incidents are well documented and maintained in order to support forensics audits, root cause analysis, and any required incident post-mortem activities.
- System-wide Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS) are implemented.

- Identity protection and integrity are maintained through the process of implementing strong authentication policies and network access controls.

To fortify the boundary transport security infrastructure, network Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS) will be placed at the boundary entry points to identify and automatically respond to signature-based threats entering and exiting the network. GDIT understands the protective attributes and benefits of a defense-in-depth approach to network security, and has applied them to formulate the MA NG9-1-1 transport security reference architecture as illustrated in Figure 20. The components of the defensible network are configured and maintained – as suggested within the NENA 75-001 guideline for the security of NG9-1-1 networks. This ensures that the prescribed security mechanisms, traffic configurations, and control points provide defense-in-depth information assurance.

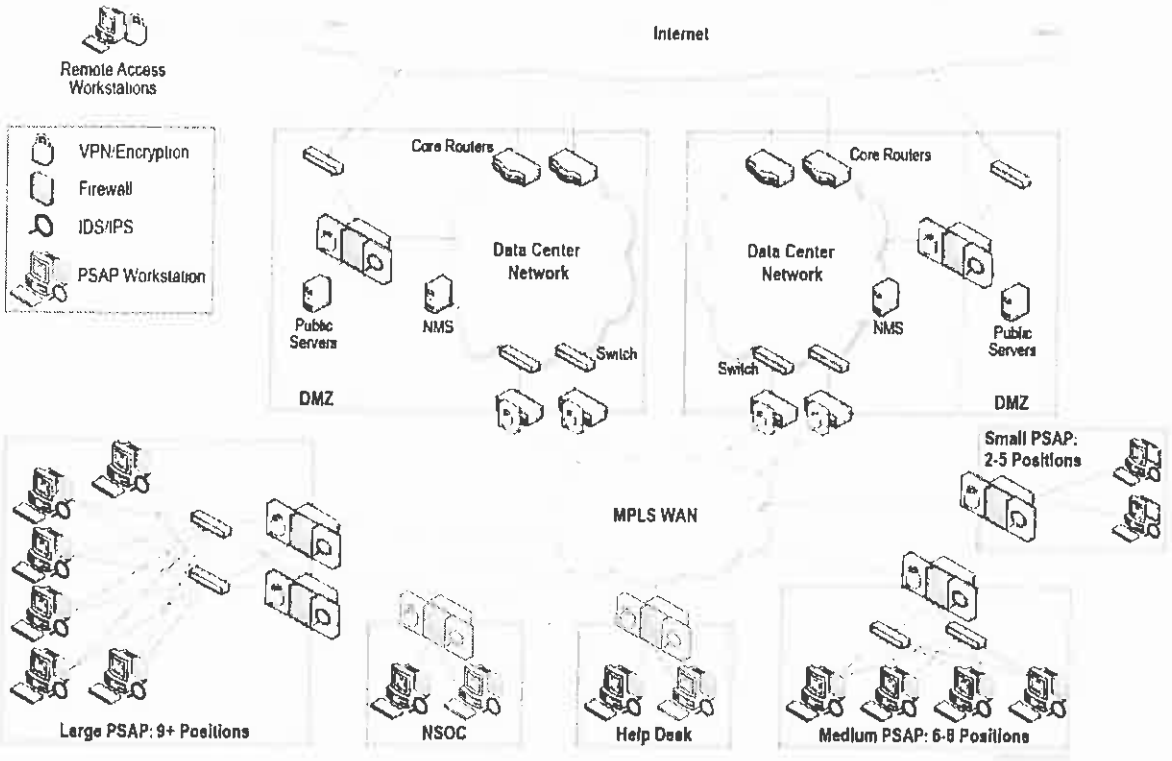


Figure 20. MA NG9-1-1 Transport Security Architecture

The MA NG9-1-1 transport security architecture houses three main security subsystems that formulate the means for secure network transmission and network security. These subsystems are:

- **Virtual Private Network (VPN)** – This subsystem is configured within the network transport architecture and will facilitate encrypted communication and network transmission for the entire MA NG9-1-1 enterprise. IP Security (IPsec) tunnels will be applied between the Cisco edge routers housed at each MA NG9-1-1 location and will formulate a point-to-point VPN mesh. The MA NG9-1-1 system will leverage encryption on all communications to ensure that data cannot be viewed or modified by anyone other

than the intended recipient as prescribed by the MA NG9-1-1 RFR. To satisfy this requirement, encryption will be applied to the network transport architecture. GDIT will configure Virtual Private Network (VPN) tunneling between each PSAP location and each data center using the integrated VPN encryption engines on the edge routers at each site. In this configuration, we propose the AES-256 advanced encryption standard, which uses a 256-bit key on all communications between locations and will ensure the security of transmissions between locations by ensuring no one is able to decipher the information should they gain access to the transmitted data. The encryption standard is Federal Information Processing Standard (FIPS) 197 compliant, ensuring compatibility with other VPN solutions. Additionally, communications by remote users to the data centers will utilize a client-based VPN, which also utilizes AES-256 encryption to ensure that only communications from authorized sources can access MA NG9-1-1 resources if required.

These VPN connections will be monitored and managed from the NSOC using a centralized Security Manager for managing a multi-device, multi-platform VPN, firewall, and IDS configuration. The manager allows these security devices to be configured and managed with an easy-to-use Graphical User Interface (GUI). It simplifies the configuration of complex VPN and security devices by creating each device's configuration file after the security policies have been defined. The Security Manager also distributes each device's configuration in a secure fashion with IPsec. It allows security devices to be configured from a central location, and it also provides other management services including monitoring, notification, and reporting.

- **Firewall** – The MA NG9-1-1 firewall capability will be rendered through the prescribed Cisco edge router configuration (part of the Cisco Security bundle) at each of the PSAP locations and the NSOC in GDIT's Needham, MA facility, as well as the data center locations facilitated by the Cisco ASA 5500 firewall. By utilizing the Cisco IOS Firewall feature set on the routers, we can ensure the network's availability and the security resources by protecting the network infrastructure against network and application-layer attacks, viruses, and worms at the edge. The Cisco firewall feature is a stateful firewall solution, certified by Common Criteria (EAL4). It also protects unified communications by guarding Session Initiation Protocol (SIP) endpoints and call control resources.

- **IPS** – The MA NG9-1-1 intrusion prevention capability will be facilitated by the Cisco IPS feature configured on each of the Cisco edge routers and ASA firewalls. IPS will operate inline, providing deep packet inspection of traffic inbound and outbound, allowing MA NG9-1-1 security analysts to accurately identify, classify, and stop or block malicious traffic in real-time.

A holistic security approach must also consider internal threats and some potential of unintended interruption of services. As such, continuous security monitoring and regular vulnerability scans and assessments are critical functions to identify, track, limit, and remediate potential threats. The least access policy concept or 'deny-by-default', in which access to only the services required to perform one's required functions, will be applied to ensure access to unneeded resources is not provided further protecting the NG9-1-1 system.

Security management is a critical component of an overall network management framework. As such, security management of the NG9-1-1 system will utilize both security and network

management tools to monitor and evaluate the status of the system at any given time. System and network device logs will be collected and evaluated to ensure the security and integrity of the system. In the event a potential incident is identified from the automated evaluation of security data, administrators at our NSOC are alerted. Once alerted, security administrators will have instant access to the desired information and will commence remediation by evaluating the incident to identify, isolate, and eliminate the threat(s) and conduct operations necessary to restore services and protect against future threats. These event and incident logs as well as change logs will be archived for future reference in case forensic or incident postmortem activities will be required.

Of particular concern in an emergency services network, is the treat of a Distributed Denial of Service (DDoS) attack. DDoS attacks are designed to create a significantly high volume of seemingly legitimate traffic usually sourced from compromised computers meant to saturate services to a state that renders the critical receiving system (edge router, file server, network, or host system) inoperable. GDIT's defense-in-depth solution provides for the best protection from DDoS attacks possible; ensuring all devices and servers have the latest security methodologies and patches installed to eliminate potential compromise. All MA NG9-1-1 devices will be secured or "hardened" to current industry best standards so that they are configured to accept traffic only on ports necessary to properly support service communications. All firewalls and routers in the MA NG9-1-1 architecture will maintain a threat defense posture and configuration that will work to eliminate potential DDoS attacks. This will be performed by filtering and eliminating traffic that is not specifically allowed on the network. Utilizing IPS throughout the architecture, with the latest signatures that are capable of identifying the most current threats, will further protect the MA NG9-1-1 network against the newest forms of attacks. Additionally, our security monitoring platform will alert on any potential threats. Working with our network provider, Windstream, this will allow us to identify and eliminate attacks as early in the communication flow as possible, thereby ensuring continuity of service for the MA NG9-1-1 network.

In its totality, the GDIT solution provides a security infrastructure that applies a variety of security measures to ensure that data theft does not occur, changes are logged and managed, data is not unintentionally modified or deleted, and identify theft does not occur. These measures include all necessary physical safeguards; operating system hardening; hardware and software information security best practices; stringent change management processes; and security incident response, resources, educational efforts, and organizational policies. This provides an environment to ensure system operations and high availability of services.

GDIT has long and extensive experience designing and managing data and voice networks to ensure a secure and defensible architecture. With network design and management contracts with the United States Marine Corps, United States Air Force, the FAA, and other federal and state organizations, GDIT is uniquely qualified to provide the expertise necessary to plan and deploy a secure emergency communications network.

8.4.2. Network Security Standards

At a minimum, the contractor shall ensure that the system complies with all applicable network security standards, including but not limited to, the following network security standards: (a) NENA Security for Next-Generation 0-1-1 Standard (NG-SEC, document 75-001 dated February 6, 2010), (b) Next Generation 0-1-1 Security (NG-SEC)Audit Checklist NENA 75-502 V1, and (c) FBI Criminal Justice Information Services (CJIS) Security Policies as set forth

on http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view and FBI Criminal Justice Information Services (CJIS) Security Policies as may be issued in the future.

GDIT complies with the RFR specification. Leveraging GDIT's security experts who designed and built the U.S. Air Force Network Security gateway system, GDIT will design, implement, and maintain the MA NG9-1-1 system in accordance with NENA security standards and the FBI CJIS security policies.

The NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) provides the minimal guidelines and requirements for protection of NG9-1-1 systems by identifying the basic requirements, standards, procedures, and practices to provide the minimum levels of security applicable to NG9-1-1.

Security Policies: as required by the NG-SEC, GDIT will work with the State 911 Department to provide applicable security documents for organizational use to provide for an effective security program of the MA NG9-1-1 system.

Information Classification and Protection: GDIT will work with the State 911 Department in the development of classification measures to protect sensitive information. Types of sensitive information can include personnel records and network configurations. Unauthorized release of sensitive information may result in lawsuits, exposed networks, and the possibility of violating federal laws.

General Security: General security is an important factor in the successful operation of any organization. Considering the critical mission of NG9-1-1 systems, GDIT staff will remain aware of and follow established security practices. Although it is not possible to eliminate all threats, implementing the steps according to NG-SEC standards can significantly aid in the reduction of those threats. A critical component in maintaining a holistic security posture will be in maintaining user-level, administrator-level, and operations-level practices that critically support security mechanisms. GDIT will work with the Commonwealth on the coordination and placement of the deployed security systems and infrastructure and the supporting practices across the Commonwealth's organizations.

Information Assets Safeguarding: Information safeguards are a function of access control. This is performed through identification, authentication, and management of these processes. Confidentiality, Integrity, and Availability (CIA) is paramount to a secure operating environment. GDIT's security measures ensure information assets such as data and network design are protected to avoid data loss and network intrusion.

Physical Security: Through physical security network devices are protected from the surrounding environment. GDIT ensures all NG9-1-1 information resources are kept physically secured and protected from theft, misappropriation, misuse, unauthorized access, and damage.

Network and Remote Access: Any access to a network has the potential to introduce malicious activity whether intentional or unintentional. All remote access to the NG9-1-1 system must adhere to security polices and security measures intended to protect the system and must not be circumvented. GDIT will ensure that all remote access provided to the network meets established business need.

Change Control and Documentation: Changes to the NG9-1-1 system can cause rippling effects throughout the network and to any other connected resources. Minor changes to a single application could cause other connected applications or network resources to stop functioning. GDIT will ensure all changes to system components are documented so that all affected parties are aware of all modifications in order to aid in troubleshooting activities. Effective change control allows all organization to know what exists in the NG9-1-1 environment and how all systems are configured.

Exception Approval and Risk Acceptance Process: Any system accessible to the public has a potential for risk. GDIT will work with the State 911 Department to manage risks associated with operation of the NG9-1-1 system. Actions taken to minimize the negative impact of identified risk demonstrates due care to protect resources including devices, data, and the ability to provide emergency services to the public. The NG-SEC standard provides an in-depth process for risk analysis, mitigation, and acceptance. Through our management process, both GDIT and the Commonwealth will be aware of the risks present and increase our ability to minimize the consequences.

Incident Response and Planning: Responding to security incidents begins with planning. GDIT will work with the State 911 Department to develop a process to detect, respond, and report security incidents. Our security monitoring will provide warning of malicious activity as it begins and will be mitigated before it has the opportunity to escalate into an incident. GDIT's experienced security personnel know what to look for and what to do when faced with a cyber security incident that will reduce system outages and the costs associated with a security breaches.

The NG9-1-1 Security (NG-SEC) Audit Checklist is a companion to the NG-SEC standard. The checklist provides a summary of the requirements and recommendations in the NG-SEC document and provides a method to document NG-SEC audits. GDIT will conduct periodic audits of the NG9-1-1 environment based on the NG-SEC Audit Checklist, and we welcome the opportunity to work with the State 911 Department on formal audits and assessments in order to obtain independent measures of the system security posture and insights for achieving a more secure environment.

The FBI's CJIS security policy establishes minimum security requirements to protect and secure various types of criminal justice information, including biometric data, identity history data, biographic data, property data, and case/incident history.

The CJIS security policy outlines a number of administrative, procedural, and technical controls that agencies must have in place to protect criminal justice information. GDIT's experience in providing secure turn-key information technology solutions to the federal government provides our team with the opportunity to support the Commonwealth in meeting these security requirements. GDIT will factor each of the following security guidelines into the MA NG9-1-1 security architecture, and we will align operational policy, procedure, and staffing needs with the functional areas associated with current CJIS security policy, which includes:

- **Information Exchange Agreements** – The information shared through communication mediums will be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums

are vital to ensuring all parties fully understand and agree to a set of security standards. GDIT will work with the State 911 Department to identify outside organizations that require interfacing to the NG9-1-1 system and establish appropriate safeguards for the sharing of information between systems.

- **Security Awareness Training** – Basic security awareness training is required for all personnel who have access to Criminal Justice Information (CJI). GDIT will work with the State 911 Department to identify personnel with access to the NG9-1-1 system who may have an occasion to access CJI. For identified personnel, GDIT will ensure appropriate security awareness training is accomplished by these personnel at the required intervals to maintain access to the system resources.

- **Incident Response** – Requires agencies to establish an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and to track, document, and report incidents to appropriate agency officials and/or authorities. GDIT's proposed solution meets the stated requirements for detecting, analyzing, containing, and recovering from security incidents. GDIT will work with the State 911 Department on reporting requirements to official inside and outside the Commonwealth that require notification of incidents.

- **Auditing and Accountability** – Requires that agencies implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. GDIT's solution provides for a complete authentication system that ensures authorized users have access to only resources required. Activities of authorized users are logged in system logs and forwarded to a central location for evaluation of inappropriate use or activities.

- **Access Control** – Access controls provide the planning and implementation of mechanisms to restrict processing and transmission of information and the modification of information systems, applications, services, and communication configurations allowing access to sensitive information. GDIT's solution provides access controls to all systems associate with the NG9-1-1 system. Access is provided only to required resources, and systems utilize multi-level access so that administrators have additional controls beyond those of system users.

- **Identification and Authentication** – Requires for the identification of information system users and processes acting on behalf of users and the authentication of the identities of those users or processes as a prerequisite to allowing access to agency information systems or services. GDIT's solution implements a fully functioning authentication framework that ensures the identity of system users and administrators and ensures authentication prior to access to any system resource.

- **Configuration Management** – Planned or unplanned changes to the hardware, software, and/or firmware components of information systems can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades and modifications. GDIT will implement a complete change and

configuration management process that ensures all proposed system modifications are tested, approved, and implemented by appropriate trained and authorized personnel.

- **Media Protection** – Requires for media protection policies and procedures to be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures will be defined for securely handling, transporting, and storing media. GDIT will work with the State 911 Department to identify all media sources for the NG9-1-1 system. GDIT will ensure only authorized personnel have physical and logical access to such media.

- **Physical Protection** – Requires that physical protection policies and procedures be documented and implemented to ensure sensitive information and information system hardware, software, and media are physically protected through access control measures. GDIT's solution ensures for the physical protection of all system resources containing sensitive information.

- **Systems and Communications Protection and Information Integrity** – Requires systems and communications safeguards including boundary and transmission protection and the securing of an agency's virtualized environment. Applications, services, and information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. GDIT's solution provides a comprehensive security infrastructure that includes all required security measures for the protection of information at system boundary and the transmission of information across external networks. Additionally, devices, servers, operating systems, and applications have additional security configurations and measures to ensure overall system integrity through detection and protection unauthorized changes and centralized logging of all system activities.

- **Formal Audits** – Formal audits are required to be conducted to ensure compliance with applicable statutes, regulations, and policies. GDIT will conduct periodic internal audits to ensure continuous compliance with all applicable policies and procedures. Additionally, we will work with the State 911 Department to conduct external formal audits as required to ensure integrity of security controls and to identify areas of potential improvement.

- **Personnel Security** – Having proper security measures against potential insider threats is a critical component for information security. Policies must be in place for all personnel who have access to unencrypted sensitive information including those individuals with only physical or logical access to devices that store, process, or transmit unencrypted sensitive information. GDIT will work with the State 911 Department to develop and implement personnel security policies to ensure that only proper individuals are given access to sensitive information and that policies are in place for administrators to enforce such policies and procedures. It should be noted that over 75% of GDIT employees already hold DoD and Federal Personal Identity Verification (PIV) security clearances.

GDIT's experienced and trained security personnel are uniquely qualified to maintain the highest level of security of the NG9-1-1 system. Our experience implementing complex enterprise

systems for the federal government provide assurance to the Commonwealth that systems under our control will remain secure and that network security standard requirements will be met.

8.5. DATA CENTERS

The system shall be supported by two (2) data centers at geo-diverse locations within the Commonwealth. The contractor shall propose two (2) data centers in diverse locations in the Commonwealth. These two (2) data centers shall meet the TIA-942 Tier 3 classification. Bidders shall describe the proposed location and the proposed support, including without limitation, identification of the space and equipment, and applications and appliances for the two (2) data centers.

Each data center shall be capable of supporting a full call load for all PSAPs throughout the Commonwealth. The call load shall be split between the two (2) or more data centers as directed by the State 911 Department. Each component of the system, including without limitation, the applications and appliances at each data center, shall meet a 99.999% standard of availability in the system architectural design. If one (1) data center becomes unavailable, all PSAP operations throughout the Commonwealth shall function off the other data center. Bidders shall describe in detail how they shall meet these requirements, including without limitation, the availability standard.

In addition, the contractor shall, within fifteen (15) business days following contract award, provide the State 911 Department with a detailed assessment of the Commonwealth data centers in Chelsea and Springfield for sufficiency with the Next Generation 911 system proposed by the contractor. The contractor shall include in such assessment a recommendation as to whether the Commonwealth data centers may be utilized to support the Next Generation 911 system. If the contractor recommends the use of the Commonwealth data centers, the State 911 Department and/or EOPSS will elect, in their sole discretion, whether to stand up the Commonwealth data centers in place of the two (2) data centers proposed by the bidder.

In addition, the bidder shall propose, as an option with separate pricing, a third, geographically diverse data center located outside of the Commonwealth. This third data center shall, at a minimum, meet the TIA-942 Tier 3 classification and TIA-942 Tier 3 recommended best practices. Bidders shall describe in detail where the originating service providers shall connect, at a point in the Commonwealth, to the third data center.

Bidders shall describe the proposed location and the proposed support, including without limitation, identification of the space and equipment, and applications and appliances of the third data center. The contractor shall describe the location of the communication service provider's demarcation point

The contractor shall implement security measures for the data centers. These measures shall include physical safeguards, operating system hardening, hardware and software information security best practices, stringent change management processes, security incident response, educational efforts and organizational policies.

Should the State 911 Department exercise the option to stand-up a third data center, said data center shall be capable of supporting a full call load for all PSAPs throughout the Commonwealth. If two (2) data centers become unavailable, all PSAP operations throughout the Commonwealth shall function off this third data center. If the State 911 Department exercises the option to stand-up a third data center, such third data center shall be maintained at one (1) software revision prior to the production system version for purposes of rolling back the system if necessary, provided that the parties mutually determine that it is feasible to do so.

The two (2) primary data centers shall be digitally cross-connected as mirror images and shall be able to operate on hot standby and/or load sharing. Bidders shall describe in detail how they shall meet this requirement for a third data center.

The contractor shall, within sixty (60) days following contract award, submit to the State 911 Department for its approval data center system design and technical documents that shall set forth all information needed to stand up the data centers, including without limitation, the HVAC, cabling electrical, and load requirements.

GDIT's proposed solution fully complies with the specified data center requirements. As part of data center readiness, GDIT will provide the Commonwealth with a data center assessment report within fifteen (15) days of contract award and submit data center system design and technical documents for Commonwealth approval within sixty (60) days of contract award.

GDIT's solution includes the placement of two geo-diverse data centers as part of the baseline deployment, with the optional deployment of a third (geo-diverse) data center. These data centers will all meet the TIA-942 Tier 3 criteria, and they will also meet a 99.999% standard of reliability. All ESInet and service-affecting components will be deployed in a high-availability configuration within each data center, and each data center will be mirrored to provide complete failover redundancy. Each data center is capable of handling the entire call volume for all PSAPs and call taker positions in the event other data center(s) becomes unavailable.

GDIT has identified two primary data centers; a Windstream facility located in Andover, Massachusetts and a colocation facility as part of the Springfield Technical Community College Assistance Corporation (Technology Park), located in Springfield, Massachusetts. GDIT believes that attaining geographical separation is important is isolating each data center from regional disasters, natural or man-made. The proposed data centers are more than 90 miles apart, with each having direct interconnection access to all major carriers and proximity to both the regionally deployed selective router pairs and to key Commonwealth technical, public safety, and executive organizations.

GDIT has partnered with Windstream to provide the transport requirement of the ESInet WAN and all telecommunications services for the Commonwealth NG9-1-1 system, including the hosted data centers. Windstream Hosted Solutions operates 27 data centers nationally, including 14 enterprise class, Tier 3 certified (TIA-942) facilities located in Boston, Philadelphia, Raleigh, Research Triangle, Charlotte, Little Rock, McLean (VA), Nashville, and Chicago, as well as many secondary markets. The enterprise class Tier 3 data centers provide 100% uptime SLAs for power and Internet connectivity due to the N+1 and 2N redundancy throughout the facilities, and both comply with SSAE#16 and Payment Card Industry (PCI) security standards. The enterprise data centers are interconnected by a fully redundant, high-capacity, facilities-based network to ensure the highest level of performance, reliability, and manageability for their clients. Windstream Hosted Solutions' data centers are designed to safeguard data and provide 100% uptime for each and every of their more than 2,500 clients.

Windstream has two Tier 3 data center facilities in Massachusetts, located in Andover and Charlestown (Boston). While both fully meet the Commonwealth's requirements, GDIT has selected Andover due to its close proximity to all critical interconnections and the selective router pairs. Furthermore, it is outside of the inherent risks and complexity of the city, including reduced congestion, accessibility, and lower public profile.

The Andover Data Center is unique in terms of Massachusetts data centers, in that it was designed and constructed exclusively as a data center. Originally owned and operated by Verizon as the 9-1-1 center for northern New England, the facility was acquired by Windstream in 2010. Subsequently, Windstream upgraded and refurbished 15 Shattuck Road at a cost of over $15M. Served by diverse, redundant feeds from National Grid and equipped with five generators that can power the city of Andover, the data center is prepared to withstand all types of man-made or natural disasters.

Key characteristics and attributes of the Andover Data Center include:

Special Building Features

- 92,700 sq. ft. data center/office building

- 40,000 sq. ft. raised floor data center area
- On-site support NOC and engineering staff 24x7
- Customer cages and private raised floor data center suites
- Disaster recovery office environment space
- Lightning protection throughout the perimeter, rooftop, electrical, and mechanical support infrastructure
- Main facility entrance requires two-factor authentication into a security "sign-in" area
- Ballistics-resistant walls, doors, and windows
- 24-inch to 36-inch raised floor rated to support 1,200 pounds/sq. ft.
- Conditioned air is supplied via the raised floor for more efficient and effective cooling of computer equipment
- Sensor-driven cameras watching every door, aisle, cage, cabinet, NOC, and other secure support rooms
- Masonry and steel construction
- Hurricane wind-rated roof
- Grounding system throughout the data center to provide connections to the raised floor, posts, cages, and cabinets

Lobby

- 24-hour physical security monitors all cameras, door positions, and badge access areas
- Redundant off-site monitoring of all security systems
- A camera on each doorway
- Double man trap forces double verification and provides extra secure data center entry and exit
- Door entrance to data center requires two-factor method authentication consisting of biometric hand scan and security code
- Biometric hand scanner verifies unique hand geometry image and a heat signature before allowing entry into the facility

Cage/Cabinet

- Cages require unique laser-etched keys with magnetic signatures
- Windstream Hosted Solutions maintains control of all keys and access to cages and cabinets requires an escort from security personnel

Electrical

- 2N or System Plus System Power design
- Four (4) pad mounted 1500 KVA service transformers (upgradeable)
- Diverse and redundant commercial power feeds from National Grid substation into all transformers

- Five (5) 1400 horsepower Caterpillar 1000kw backup generators
- Two (2) 15,000 gallon double wall fiberglass underground fuel storage tanks
- Contracts with multiple fuel vendors
- Generators tested weekly at no load and quarterly at full load
- Four (4) GE 500kw Uninterrupted Power Supply (UPS) inverters and battery packs; N + 1 configuration (scalable to 12 units)

HVAC

- 24-inch raised floor and drop ceiling for efficient air handling
- Environmentally friendly cooling towers and condensed water pump system
- Chilling plant with a combination of centrifugal and reciprocating chillers
- Plate heat exchanger unit
- Computer Room Air Handler (CRAH) units throughout the data center for air handling
- Water detection system (Liebert Leak Detection) below the floor of the data center

Building Management Systems

- Foreseer and Java Application Control Engine (JACE) building management systems monitor all critical facility infrastructure
- Leak detection systems throughout the facility

Security Cameras

- Video surveillance and capture to Digital Video Recorder (DVR)
- 24-hour physical security monitors all cameras, door positions, and badge access areas
- Redundant off-site monitoring of all security systems
- Cameras at each doorway and Pan-Tilt-Zoom (PTZ) cameras throughout the exterior of the facility

Access Controls

- 24x7 on-site personnel
- Card-reader access system
- Biometric identity access system
- Electronic verification by Windstream Hosted Solutions personnel
- Individual cabinet combination locks

The second proposed data center is a Windstream shared facility operated by the Springfield Technical Community College Assistance Corporation located at 1 Federal Street in Springfield. Referred to as Technology Park, the facility was established in 1996 with funding from the Commonwealth of Massachusetts, and with operations overseen by a board of directors. Technology Park is the premier complex in Western Massachusetts for clients seeking a "totally smart" environment in which to locate their operations. Tenant companies have invested in excess of $300 million in equipment and technology in the Park, including fiber, telecommunications networks, and switching equipment.

Technology Park serves as the telecommunications hub of Western Massachusetts, providing interconnection to most primary carriers, including Axia/Massachusetts Broadband Initiative. Technology Park is also strategically located in close proximity to the Commonwealth data center at 53 Eliot St., reducing engineering considerations should the Commonwealth choose to use their 53 Eliot St. facility in place of the Technology Park facility. Technology Park is also located in close proximity to the westernmost selective routers, reducing TDM backhaul complexity.

Windstream presently has interconnection within Technology Park, providing direct access to the Windstream 'Core', Furthermore, Windstream has existing redundant, diverse 1 GB connections between Technology Park and the 53 Eliot St. facility.

Technology Park is presently undergoing renovation, that will bring the facility into Tier 3 compliance. Should the Commonwealth select this location, the renovations are committed to be completed in January 2015, prior to services going live. Windstream applies its proven experience and capabilities in delivering high-reliability, high-security hosted solutions in preparing and managing the 1 Federal Street space.

Key characteristics and attributes of the Springfield 1 Federal Street facility include:

Special Building Features

- 65,000 sq. ft. data/office building
- 40,000 sq. ft. of raised floor data center area
- On-site support NOC and engineering staff 24x7
- Customer cages and private raised floor data center suites
- Lightning protection throughout the perimeter, rooftop, electrical, and mechanical support infrastructure
- Main facility entrance requires two factor authentication into a security 'sign-in' area
- Ballistics-resistant walls, doors and windows
- 24-inch raised floor rated to support 1,200 lbs./sq. ft.
- Conditioned air is supplied via the raised floor for more efficient and effective cooling of computer equipment
- Sensor-driven cameras watching every door, aisle, cage, cabinet, NOC and other secure support rooms
- Masonry and steel construction
- Hurricane wind-rated roof
- Grounding system throughout the data center to provide connections to the raised floor, posts, cages and cabinets

Lobby

- 24-hour physical security monitors all cameras, door position, and badge access areas
- Redundant off-site monitoring of all security systems

- A camera on each doorway
- Double man trap forces double verification and provides extra secure data center entry and exit
- Door entrance to data center requires two-factor method authentication consisting of biometric hand scan and security code
- Biometric hand scanner verifies unique hand geometry image and a heat signature before allowing entry into the facility

Cage/Cabinet

- Cages require unique laser-etched keys with magnetic signatures
- Windstream Hosted Solutions maintains control of all keys and access to cages and cabinets require an escort from security personnel
- Strong sheet metal cages with no hand and foot holds are available for larger deployments

Electrical

- Fully 2N A-side and B-side power distribution design
- Automated failover between electrical systems
- 6,000 kVA of utility capacity
- Upstream utility switching between substations
- Four 1MW Cummings/Katolite generators with 24,600 gallons of fuel capacity
- Partnerships with multiple fuel vendors for fuel delivery
- Generators tested weekly at no load, monthly load bank test and quarterly facility transfer
- Redundant A-side and B-side ASCO 7000 series Automatic Transfer Switches (ATS)
- Both the A-side and B-side electrical systems have two paralleled 750kVA high-efficiency GE Uninterrupted Power Supply (UPS) systems per side
- Total of four (4) 750 kVA GE UPS systems expandable to eight (8)
- True 2N UPS redundancy in each electrical system
- 1,215 kW of usable UPS capacity expandable to 2,430 kW
- A-side and B-side ATS, main switchboards, UPS systems and Power Distribution Units (PDU)
- The fast detection and switching capability of the Static Switch (STS) PDU (<4ms) allow for uninterrupted power (even for single power-supplied equipment)
- Each customer cabinet will have redundant A-side and B-side power feeds
- Mechanical plant supported by Active Power Rotary UPS

HVAC

- 2N cooling tower redundancy
- 2N chilled water pump redundancy
- N + 1 chiller redundancy

- N backup DX air cooled chiller
- Dual loop chilled water
- N + 1 CRAH units dual fed from A-side and B-side sources

Building Management Systems

- Foreseer and JACE building management systems monitor all critical facility infrastructure
- Dry-pipe, pre-action sprinkler
- Multi-zoned smoke/heat detection system
- Leak detection systems throughout the facility

Security Cameras

- Video surveillance and capture to DVR
- 24-hour physical security monitors all cameras, door positions, and badge access areas
- Redundant off-site monitoring of all security systems
- Cameras at each doorway and Pan-Tilt-Zoom (PTZ) cameras throughout the exterior of the facility

Access Controls

- 24x7 on-site personnel
- Card-reader access system
- Biometric identity access system
- Electronic verification by facility personnel
- Individual cabinet combination locks

The ESInet WAN bandwidth at each of the primary data centers in the Commonwealth has been calculated to fully support over 100% of the traffic demands for the entire NG9-1-1 environment at each data center, on each of the two redundant 1GB circuits. The load balanced connections from each of the data centers will enter the Windstream MPLS WAN Core and then link to all of the PSAPs, Training Centers, and Police/Fire facilities to support ESInet routing of all NG9-1-1 services, and to the GDIT NSOC to provide operations and management.

Third Data Center

GDIT proposes an out-of-state third data center using the Windstream Tier 3 facility in McLean, VA. As articulated in Section 8.7.1 (Routing Requests), GDIT believes a third data center is best considered for deployment when most or all carriers agree to IP-based Network-Network Interface (NNI) for egress traffic, vastly simplifying the duplication and transport of traffic. The third facility would implement the same network architecture as Data Center I and Data Center II, and offer a fully mirrored set of systems and capabilities.

The third, geographically diverse, data center proposed is Windstream Hosted Solutions McLean Data Center located 1764-A Old Meadow Lane in McLean, VA. The McLean Data Center came online in March 2013, and is designed and implemented to meet the TIA-942 Tier 3 and SAE-16 Type2 standards as well as PCI and Health Insurance Portability and Accountability Act

(HIPAA) compliance. The facility, as well as the overall design of the components, will meet the 99.999% standard of availability in the system architectural design as well as the TIA-942 Tier 3 classification and TIA-942 recommended best practices.

Key characteristics and attributes of the McLean facility include:

Special Building Features

- 65,000 sq. ft. data/office building
- 40,000 sq. ft. of raised floor data center area
- On-site support NOC and engineering staff 24x7
- Customer cages and private raised floor data center suites
- Lightning protection throughout the perimeter, rooftop, electrical, and mechanical support infrastructure
- Main facility entrance requires two factor authentication into a security 'sign-in' area
- Ballistics-resistant walls, doors and windows
- 24-inch raised floor rated to support 1,200 lbs./sq. ft.
- Conditioned air is supplied via the raised floor for more efficient and effective cooling of computer equipment
- Sensor-driven cameras watching every door, aisle, cage, cabinet, NOC, and other secure support rooms
- Masonry and steel construction
- Hurricane wind-rated roof
- Grounding system throughout the data center to provide connections to the raised floor, posts, cages, and cabinets

Lobby

- 24-hour physical security monitors all cameras, door position, and badge access areas
- Redundant off-site monitoring of all security systems
- A camera on each doorway
- Double man trap forces double verification and provides extra secure data center entry and exit
- Door entrance to data center requires two-factor method authentication consisting of biometric hand scan and security code
- Biometric hand scanner verifies unique hand geometry image and a heat signature before allowing entry into the facility

Cage/Cabinet

- Cages require unique laser-etched keys with magnetic signatures
- Windstream Hosted Solutions maintains control of all keys and access to cages and cabinets require an escort from security personnel

Electrical

- Fully 2N A-side and B-side power distribution design
- Automated failover between electrical systems
- 6000kVA of utility capacity
- Upstream utility switching between substations
- Four 1MW Cummings/Katolite generators with 24,600 gallons of fuel capacity
- Partnerships with multiple fuel vendors for fuel delivery
- Generators tested weekly at no load, monthly load bank test and quarterly facility transfer
- Redundant A-side and B-side ASCO 7000 series Automatic Transfer Switches (ATS)
- Both the A-side and B-side electrical systems have two paralleled 750kVA high-efficiency GE Uninterrupted Power Supply (UPS) systems per side
- Total of four (4) 750kVA GE UPS systems expandable to eight (8)
- True 2N UPS redundancy in each electrical system
- 1215kW of usable UPS capacity expandable to 2430kW
- A-side and B-side ATS, main switchboards, UPS systems and Power Distribution Units (PDU)
- The fast detection and switching capability of the Static Switch (STS) PDU (<4ms) allow for uninterrupted power (even for single power-supplied equipment)
- Each customer cabinet will have redundant A-side and B-side power feeds
- Mechanical plant supported by Active Power Rotary UPS

HVAC

- 2N cooling tower redundancy
- 2N chilled water pump redundancy
- N + 1 chiller redundancy
- N backup DX air cooled chiller
- Dual loop chilled water
- N + 1 CRAH units dual fed from A-side and B-side sources

Building Management Systems

- Foreseer and Java Application Control Engine (JACE) building management systems monitor all critical facility infrastructure
- Dry-pipe, pre-action sprinkler
- Multi-zoned smoke/heat detection system
- Leak detection systems throughout the facility

Security Cameras

- Video surveillance and capture to DVR
- 24-hour physical security monitors all cameras, door positions and badge access areas

- Redundant off-site monitoring of all security systems
- Cameras at each doorway and Pan-Tilt-Zoom (PTZ) cameras throughout the exterior of the facility

Access Controls

- 24x7 on-site personnel
- Card-reader access system
- Biometric identity access system
- Electronic verification by Windstream Hosted Solutions personnel
- Individual cabinet combination locks

Cabinets

- All Standard cabinets are a 42U Tripp-Lite cabinet
- 40U Usable. 73.5" in height
- Four (4) interior vertical posts with unthreaded square hole openings
- Standard 24" width (19" usable) and 42" depth

Standard Cages

- A standard "Newton" cage is 94.5" in height. Consists of two (2) 27" width doors placed in a hot and cold aisle
- 8x8 cage (64 square feet) and can accommodate four (4) 42U Trip-Lite cabinets.
- 8x10 cage (80 square feet) can accommodate five (5) 42U Trip-Lite cabinets.

GDIT's proposed solution includes a point-to-point connection between data centers that will be carried over 10 Gigabit wavelength transport for the purpose of:

- Synchronizing databases, configurations and system state over a private, highly available and low latency connection.
- Allow for application layer failover
- Replicating data for storage
- Providing an alternate path to each data center should the primary, redundant 1GB ESInet connections fail

Connectivity

The initial phase of deployment will provide a 10 Gigabit connection between the two initial data centers. Windstream has the ability to deploy a "fiber ring" encompassing the proposed third data center facility and would traverse geographically diverse transports from East to West within the Commonwealth.

When the Commonwealth deploys a third out-of-state data center in the Windstream McLean, VA Data Center, the facility would maintain the same network architecture as the Data Center I and Data Center II. Windstream will have the ability to provide 10 Gigabit wavelength connection from the third data center to both the Springfield, MA and Andover, MA data centers.

Windstream will also provide off-network PSTN SIP trunks for administrative calling. 100 SIP trunks will be provided at each data center and will be configured for inbound and outbound calling in addition to, or in place of, local PSTN trunks.

8.5.1. Data Center Network Bandwidth

Bidders shall describe in detail the bandwidth and redundancy recommended at the two (2) data centers and any third data center to provide 99.999% system availability. These network connections shall support ESInet connections to the PSAPs, data centers, carrier PoPs, communication service provider connections, and other ESInets.

The contractor shall identify the required bandwidth to handle anticipated traffic, including the following: 1) the aggregated ESInet connections to PSAPs; 2) connections between data centers. 3) connections to the public Internet; 4) connections to communications service providers, via traditional trunks and private IP circuits; 5) connections to legacy PSAPs; 6) connections to existing selective routers; and 7) any other connections that may be required. This shall include provisions for redundancy and anticipated growth as new payload types are introduced to the system. Bidders shall include in their calculation how they arrived at these bandwidth requirements.

The contractor shall describe in detail the specifications for the data center network connectivity, architecture, and physical requirements.

The system shall connect to private safety departments currently operating on the legacy system, and the system shall connect to legacy and Next Generation 911 CPE for secondary PSAPs and limited secondary PSAPs. The State 911 Department does not furnish CPE for the private safety departments. Currently, the State 911 Department provides CPE for the following secondary PSAPs only: Boston Fire Alarm, Springfield Fire, and Worcester Fire. The private safety departments currently operating on the legacy system, and the current secondary PSAPs are identified on Attachment G- Secondary PSAP Data. The current limited secondary PSAPS are identified on Attachment H- Limited Secondary PSAP Data.

The contractor shall recommend an alternate network transport for the system.

GDIT's proposed ESInet solution is entirely packet based and fully modular in design. All traffic within the ESInet and remote sites is IP and is delivered via the Ethernet, with the possible exception of ingress traffic from carriers and identified off-network (PSTN) trunks at local PSAPs. Each PSAP connects to the ESInet utilizing Cisco edge router(s) and delivers IP traffic to the call taking positions and supporting systems.

The follow connection bandwidth and calculation criteria have been used to determine bandwidth requirements:

- **PSAP ESInet** – Bandwidth for each PSAP has been calculated based on 750k required per call taker position, with each position assumed to be active simultaneously. Actual minimum requirements are 512k per position, but 750k was utilized as a best-value approach to meet probable growth demands in services (payload types), position, and mapping demands. A breakdown of the 512k minimum is shown in Section 8.7, Next Generation 9-1-1 Architecture.

- **Aggregate ESInet** – All ESInet traffic is assumed to occur between each data center and each PSAP, including on-net PSAP-to-PSAP traffic. With 830 existing call taker positions and a minimum bandwidth requirement of 512k per position, a minimum connection to each data center is approximately 425 MB. Using the best value of 750k per position, each data center requires approximately 640 MB. GDIT's proposal includes redundant 1 GB lines between data centers and the ESInet.

- **Data Centers** – GDIT has provided 10 GB redundant connections between the two data centers (and optionally the third data center). This connection will be used for database and systems synchronization, replication, and alternate network routing in the event of ESInet WAN or application failure. The minimum required bandwidth to support these functions is 1 GB for each data center sharing the bandwidth (e.g., 2 GB for two data centers).

- **Public Internet** – Public connections are provided in the DMZ of each data center to allow remote user connectivity, remote operations and management, update and patch management, and reporting. If PSAP connections to MBI are selected for NG9-1-1, secondary PSAP connections by the Commonwealth, these services will egress the ESInet through direct connections to MBI and the Windstream WAN Core, and they will not use the DMZ. A minimum of 20 MB has been provided in each data center.

- **Carrier** – Definition of ingress 9-1-1 traffic from carriers is a critical component of the transitional environment, as discussed in Section 8.7.1 (Routing Requests). GDIT assumes that each carrier will be responsible for terminating their traffic at the redundant data centers as part of the FCC ruling on public safety termination. The bandwidth required will be based on 64k per connection for TDM traffic and 92k for IP (SIP) connection. The number of connections is based on ERLANG B calculations provided on a per-carrier basis utilizing traffic volume and subscriber counts.

- **Legacy PSAP** – Commonwealth Public Safety departments or other sites that will not upgrade console positions are expected to remain served by the selective router and would not require an ESInet connection. Should the selective router connection to these sites be moved to the data centers, an ESInet connection would be required and a legacy PSAP gateway placed locally until such time as the E9-1-1 console is replaced with an NG9-1-1 position. The bandwidth required to support a LPG will be 256k per console position.

- **Selective Router** – As identified in Section 8.7.1, the use of the selective router to direct services requires that each trunk be duplicated and forwarded to each data center. How the incumbent will allow Network-to-Network Interfaces (NNI), including the use of CAMA, T1, SS7, or IP, will be subject to discussions with the incumbent. As with the carrier connections, the bandwidth required will depend on the termination type, interface, and ERLANG B calculations.

- **Data Center Off-net** – GDIT's solution utilizes both (or either) a local PSAP trunk or a data center trunk to provide administrative inbound or outbound calling. Where centralized (data center) calling is used, GDIT has provided 100 SIP trunks at each data center for shared use across all administrative phones.

Additionally, each limited secondary PSAP is proposed to support ESInet connectivity utilizing a T1 (1.5 MB) leased connection. Given the mission of this type of site, it is recommended to use the existing Internet connections, saving cost of the T1 connection. The availability and performance of this connection would need to be assessed if the Internet connection is not managed, although it is expected that an MBI connection will support appropriate traffic engineering.

8.6. GEOGRAPHIC INFORMATION SYSTEMS

Through MassGIS, the Commonwealth has created a comprehensive, statewide database of geospatial information. MassGIS is the official Massachusetts state agency responsible for the collection, storage and dissemination of geographic data. In addition, MassGIS is responsible for coordinating geographic information system activity within the Commonwealth and setting standards for geographic data to ensure universal compatibility. MassGIS will be the source of the GIS data that shall be used for the deployment of the system. The contractor may be required to enter into appropriate non-disclosure or license agreements with a third party database provider, MassGIS, and/or or other parties.

Next Generation 911 depends on Geographic Information System technology and i3-compliant spatial data for a number of functions, including but not limited to, call routing, location validation, and determining the appropriate public safety agency that is responsible for an incident's location. The Commonwealth will provide to the contractor the set of i3-compliant spatial datasets necessary for these functions to operate throughout the Commonwealth. This section of the RFR briefly describes the data available from the Commonwealth.

Bidders shall not bid on the provision of GIS data, and cost proposals shall NOT include provision of GIS data other than as expressly set forth herein.

All GIS data shall remain the exclusive property of the Commonwealth, including without limitation, any derivatives that the contractor may produce.

The following spatial datasets will be made available to the contractor to be used by the system. All data will be provided in i3-compliant format and will contain all required i3 spatial attributes. Data sets will be provided on a regional basis (except that data sets for wireless state police PSAPs will be provided on a statewide basis).

GDIT will utilize the MassGIS-provided spatial datasets and will provide a compliant GIS solution to include GIS data normalization services. As requested, out proposal does not include the provisioning of GIS data.

The spatial datasets provided by the Commonwealth will be analyzed when received and feedback will be provided to the Commonwealth. Detailed analysis and data normalization will be performed, as detailed in Section 8.7.14 (Spatial Information Function) and Section 8.7.23 (Mapping). As the datasets will be provided on a regional basis, with the exception of the wireless State Police PSAPs, which will be provided on a statewide basis, this breakdown will be evaluated as a means to use a Location-to-Service Translation (LoST) tree rather than a single state-wide ECRF.

The GDIT team is prepared, if required, to enter into appropriate non-disclosure or license agreements with a third-party database provider, MassGIS, and/or other parties.

8.6.1. Polygon Boundaries

The Commonwealth will provide to the contractor the following polygon boundaries, derived from a map of ESNs:

Public Safety Answering Point Boundaries – non-overlapping boundaries in i3- compatible format for PSAPs throughout the Commonwealth;

Fire service agency boundaries – non-overlapping boundaries in i3-compatible format for fire departments throughout the Commonwealth;

Law enforcement service agency boundaries – non-overlapping boundaries in i3- compatible format for all local, regional, and state law enforcement agencies (police and sheriff departments) throughout the Commonwealth; and

Emergency Medical Services agency boundaries – non-overlapping boundaries in i3- compatible format for all emergency medical services agencies throughout the Commonwealth.

The Commonwealth will also provide to the contractor:

- *MSAG community boundaries, within which number/street name are unique (with a handful of exceptions statewide); and*

- *Authoritative municipal and state boundaries.*

The GDIT team will evaluate the PSAP boundary file for use as the default SOS service boundary layer. Fire, law, and EMS layers will be evaluated for use as sub-service layers (e.g., sos.police). All relevant boundary layers will be used as part of the data normalization process to assist in the various quality control processes as detailed in Section 8.6.7, GIS Data Normalization Services.

8.6.2. Street Segment File

The Commonwealth will provide to the contractor a complete street centerline file that covers the entire Commonwealth and towns immediately adjacent to the Commonwealth in other states. This file contains a link from each segment to address ranges, street names and alias street names, and other i3-required attributes, along with i3-compatible coordinates. Where street segments intersect the polygon boundaries referenced above, the segments will be split to contain appropriate address ranges on both sides of the split.

The GDIT team will utilize the street centerline file to provide the base geocoding services within the ECRF/LVF as well as the call taking map display. It will also be used in the data normalization process.

8.6.3. Point Address Locations from Structure Polygons

The Commonwealth will provide a point file of address locations. All structures in the Commonwealth have been mapped as of 2011 and each structure polygon is associated with one or more address points. The structures layer is being maintained on an annual basis using aerial photo. The address points include parcel centroids, non-building locations such as parking lots or playing fields, as well as structure-derived centroids, entry points and/or interior points. Almost all address points link to one or more address listings in a master list compiled from and being maintained in sync with various sources including the ESL, the statewide voter list, building permits, local tax lists and other sources such as utility customer lists. All the civic style address records in this master list, from whatever source, have had their number and street name standardized to meet NENA-specified format and to cross-reference other address records. Address records which have no matching point locations are being identified and points which are associated with structures but have no address will be linked by local officials to address points using a field data collection application. Future maintenance of this point layer will be delegated to local or regional stakeholders.

The GDIT team will utilize the point file of address locations to provide the base geocoding services within the ECRF/LVF and the call taking map display. As this dataset is potentially incomplete, the street centerline file will be used to locate address locations not available in this layer.

8.6.4. Other Spatial Data

The Commonwealth will provide to the contractor additional data maintained by MassGIS if required, upon such terms and conditions as may be negotiated with the contractor. These include, but are not limited to, aerial photographs, digital terrain maps, tax parcel boundaries, hydrologic and other features. All of these datasets can be provided in native file formats or in ESRI database formats as appropriate. MassGIS may organize the data into regional, PSAP, and Commonwealth-wide datasets. The contractor may also wish to access web mapping services for MassGIS-provided, tiled, cached basemap display (see Section 8.6.6).

The GDIT team will evaluate the usefulness of the additional spatial data available from MassGIS and proceed accordingly. Although these additional layers will not be required by the ECRF/LVF, they would potentially be of value in the call taker's map display.

8.6.5. Sample Spatial Data

MassGIS will develop a set of sample datasets that are representative of the Commonwealth-wide spatial data described above and other layers relevant to the Next Generation 911 deployment. Some of these datasets are

currently available on the MassGIS website at www.mass.gov/mgis and others can be made available to the contractor as ESRI datasets or in an Open Geospatial Consortium's i3-compatible Geography Markup Language with associated i3-required attributes or as web services using either ESRI or OGC-compatible request formats. The sample datasets will include a mix of urban and rural areas of the Commonwealth, in a contiguous format, to enable the contractor to determine the complexity and breadth of the spatial data that shall be supported. The sample data sets will include a subset of all of the datasets that will be provided to the contractor.

The GDIT team will access and examine the sample spatial datasets and load them into test systems for further evaluation. The datasets will be tested through the Signaling Information Field (SIF), quality control, to the ECRF/LVF.

8.6.6. Orthophoto Interface

The system shall have a web services or other interface to tiled, cached, orthoimages and basemapping using either OGC or ESRI compatible request formats. Bidders shall describe such functionality, where the cached imagery and basemapping will reside and shall describe update and maintenance workflows.

Included in the proposal are both client-side and server-side mapping components. Each data center will host a redundant ArcGIS server pair, serving read-only map services for use by the call taker map display. These map services can serve tile-based displays with or without orthophotos. ESRI Locator web services will also be used to allow call takers to look up addresses, intersections, and other map data (common places for example). The call taker display will also utilize the ESRI Locator services upon receipt of a new 9-1-1 call that contains a civic address (with PIDF-LO), locating the caller on the map.

Alternatively, the call taker map can be configured to use ESRI-based web services provisioned by MassGIS. In this scenario, DDTi would require tile-based services (with and without orthophotography), and ESRI Locator services. Availability and connectivity to the MassGIS will need to be determined in this scenario.

The call taker map display is built on the ESRI Windows Presentation Foundation (WPF) runtime. It can accept the services provided by ArcGIS server and present maps, with or without orthophotography, to the call takers. Optionally, the call taker map display call pull map packages from the ArcGIS server periodically, and use these packages locally.

If the Commonwealth opts to have the ArcGIS server implementation within the ESInet, it will pull the map data directly from the DDTi Data Manager NXG solution in order to build the map tiles. Map tiles will be built on a recurring schedule to keep them as up to date as possible. The tiles will be stored on the ArcGIS server hardware, and served up to the call taker map display as needed. The call taker map display will cache received tiles locally, and only request tiles from the server for areas not in the local cache (or if the tiles in the local cache are out of date). DDTi recommends using an ArcGIS server implementation within the ESInet that is directly tied to DDTi Data Manager NXG for data consistency purposes. As an example, if MassGIS serves out all roads to the call taker's map display, it may include roads that fail quality control in DDTi Data Manager NXG, meaning the call taker's map will not be synchronized with other map data within the ESInet (in the ECRF for example). If ArcGIS server map services are tied directly to DDTi Data Manager NXG, then it provides assurances that the map data the call taker is working with is exactly the same map data used elsewhere within the ESInet.

8.6.7. GIS Data Normalization Services

The contractor shall provide GIS data normalization services. Bidders shall propose processes and pricing to work collaboratively with MassGIS to normalize all GIS data to be used within the system. Bids shall include the specification of both mandatory and optional/recommended GIS datasets required for implementation and all required schemas and data structures. The contractor shall work with MassGIS to develop extract, transform and load routines to populate system tables from existing datasets. The current data model related to Next Generation 911 matching is set forth in Attachment I- GIS Data and Data Scheme.

In addition, the contractor shall provide quality assurance and control services to include review of the following, at a minimum:

- *Missing data layers;*
- *Missing attribute information;*
- *Standardization of GIS data attributes in adherence to relevant national standards, both centerline and site/structure location points following the FGDC-STD-016-2011, NENA GIS Data Model, NENA Site Structure Address Point;*
- *Synchronization of GIS data with MSAG and ALI (NENA 71-501 v1). MassGIS street centerline is currently being maintained at 99% or better level of synchronization with MSAG;*
- *Address range parity in centerline, as well as relating to site/structure location points and centerline;*
- *Duplicate address ranges;*
- *Direction and flow errors;*
- *Gaps and overlaps in PSAP and service boundaries and edge matching; and*
- *Centerline breaks at intersections and boundaries.*

In addition, the contractor shall work with MassGIS to develop a strategy to ensure timely and accurate local input of address information and any other changes to the key datasets required for Next Generation 911 operation.

GIS data normalization is a process by which (potentially) disparate GIS/location datasets are checked, groomed, and formatted such that they can be accurately merged into a single, common, and authoritative database. The GDIT team structures its data normalization process into four main areas:

1. **Data Quality Control** – these activities help establish organizational policy guidelines and principles to ensure the integrity and accuracy of the data.
2. **Internal System Data Synchronization** – these activities are associated with the design, configuration, testing, and acceptance that the two systems (MassGIS and ArcGIS) are communicating properly to exchange and synchronize data with test trial data.
3. **Addressing Information Synchronization** – these activities include the synchronization of centerline / ALI, centerline/ Master Street Address Guide (MSAG), ALI/ address points, and MSAG/ address synchronization.
4. **Spatial and Boundary Synchronization**, which synchronizes address information with spatial and boundary capabilities to enable the use of polygons.

GDIT applies a closed loop (Test → Correct → Test) approach for each of the above GIS data normalization areas to ensure the data meets the specified requirements.

The precise steps necessary to make GIS data usable in a NG9-1-1 environment will vary with the quality and completeness of the data. The GDIT team will first assess the availability and structure of the existing GIS data (as outlined in NENA 02-010 and with consideration toward NENA's NG9-1-1 GIS Data Model). NENA's NG9-1-1 GIS Data Model will define the

minimum layers required and minimum field requirements that must be populated for functionality in both the ECRF and LVF.

NENA's initiative for developing an informational document to support the development of spatial placement of GIS address points (NENA Site Structure Address Point) is meant to guide addressing authorities with recommendations on the development of address points and placement techniques. This document mainly takes into consideration the data's usage in public safety applications, consideration of access locations versus building locations, and address placement guidelines based on numerous real-world scenarios. This document is not intended to serve as a guideline for completeness or accuracy of the supporting data behind the GIS, but rather describes how to make informed decisions for numerous methodologies of creation and modification of GIS address placement.

Minimum NENA Data Requirements

In NG9-1-1, NENA's definition (NG9-1-1 GIS Data Model and NENA 08-003 v1) for Emergency Service Zones (ESZs) has been replaced by Service Boundaries. The Service Boundaries are similar to ESZs in that they serve as services available for call routing and dispatching. For transitional purposes, comparisons to the ESZs will be used for testing and evaluating the accuracy of topology and attributes. Geocoding the MSAG and ALI to the road networks will determine where there are inconsistencies in any layer.

Road centerlines are required, and must include the following minimum attributes:

- An integer unique ID
- Name fields, including prefix, name, type, and suffix
- Political division fields, including state, county (or equivalent), and incorporated municipality (if applicable), each for both left and right sides of the road
- Address range to/from values for both left and right sides of the road

Address site/structure points are not required, but strongly recommended. They must include the following minimum attributes:

- An integer unique ID
- An integer house number with one of the following:
  - Name and political division fields, including street prefix, name, type, and suffix, state, county (or equivalent), and incorporated municipality (if applicable), OR
  - A reference unique ID and side field, indicating a road centerline from which to inherit the name and political division fields

A service boundary layer (polygons) is required for each service that is to be used. Attributes required for NG9-1-1 include:

- Display name
- Service number
- SIP Uniform Resource Identifier (URI)

Attributes required for E9-1-1:

- Emergency Service Number
- Fire
- Emergency Management System (EMS)
- Law
- Or other responding agency

FGDC Standard (FGDC-STD-016-2011)

In addition to the NENA standards, the Federal Geographic Data Committee (FGDC) has established standards contained in the United States Thoroughfare, Landmark, and Postal Address Data Standard publication. The following table has been generated from Part 4 Addressing Data Quality and Appendix G. While we will run other Quality Control (QC) tests for the data that are not described in the document, these tests from FGDC will be completed as part of the Data Quality and/or Data Synchronization phase. The designation of "Optional" indicates tests will be run if the data contains these data elements.

Table 4. FGDC Addressing Quality Control

Test Name	Road Centerlines	Address Points	ALI	MSAG	ESN Polygons	MSAG Polygons	Address System
Address Completeness		X					
Address Elevation		X					
Address Left Right		X					
Address Life Cycle Status Date		Optional					
Address Number Fishbone	X	X					
Address Number Parity		X					
Address Number Range Completeness	X			X			
Address Range Directionality	X						
Address Reference System Axes							Optional
Address Reference System Rules							Optional
Check Attached Pairs							
Complex Element Sequence Number		Optional					
Data Type	X	X	X	X	X	X	Optional
Delivery Address Type Sub-Address		Optional					
Duplicate Street Name	X						
Element Sequence Number		Optional					
Future Date	Optional	Optional	Optional	Optional	Optional	Optional	Optional
Intersection Validity	X						
Left Right Odd Even	X	X					
Location Description							
Low High Address				Optional			

Test Name	Road Centerlines	Address Points	ALI	MSAG	ESN Polygons	MSAG Polygons	Address System
Sequence							
Official Status Addressing Authority Consistency	Optional	Optional					
Overlapping Ranges	X			X			
Pattern Sequence		Optional					
Range Domain	X			X			
Related Element Uniqueness	Optional	Optional					
Related Element Value	Optional	Optional					
Related Not Null	Optional	Optional					
Segment Directionality Consistency	X						
Spatial Domain	X	X			X	X	
Start End Date	Optional	Optional	Optional	Optional	Optional	Optional	
Sub-Address Component Order		Optional					
Tabular Domain	X	X	X	X	X	X	
Uniqueness Measure	X	X	Optional	Optional	Optional	Optional	
USNG Coordinates		Optional					
XY Coordinate Completeness	X	X			X	X	
XY Coordinate Spatial	X	X			X	X	

Data Quality Assurance and Control Phase

Once the source data meets these minimum requirements, the GDIT team will map all possible fields for import into the automated QC process. Following import, the system will perform additional QC checks for topology and attribute consistency and produce documentation on the various errors and warnings. Where applicable, the documentation will have X and Y coordinates for spatial representation in GIS software to represent the data discrepancy along with a location for remediation.

The GDIT team's GIS analysts will provide this information in the requested format with specific recommendations for corrective actions to be made by the designated parties.

Additional QC will take place when the MSAG and ALI validation routines are run, providing a report of the mismatches. Past processing of this validation indicates most errors will be in the ALI database, but this report can provide useful information for fixing the GIS data when necessary.

Comparison of civic locations to the ALI is intended to significantly reduce or eliminate the chance for errors during actual emergency calls for E9-1-1. In NG9-1-1, civic locations are pre-validated against the LVF.

The goal of geocoding is to unambiguously determine the location of a caller using the data that is available at the time of query. The quality, completeness, and integrity of the data used will obviously be a factor in the outcome of this process and could ultimately mean the difference between life and death when it comes to public safety.

In NG9-1-1, the LoST server (ECRF and LVF) geocodes all Civic Address queries in order to compare the geographic location to service boundary polygons. Addresses are considered to have a highest quality rating and will be checked against first before looking for potential road centerline matches. This process ultimately results in a call routing URI in the LoST response.

Data Requirements

The processes outlines assume that we have the following data: the GIS data formatted as outlined in Attachment I; the ALI data formatted as outlined in Attachment J; and the tabular MSAG data formatted in compliance with NENA 71-501. Ortho photography data is highly recommended to facilitate the Data Quality Control.

Auxiliary Data

As expressed in NENA 02-014, the use of tax assessment information, ALI, MSAG, Utility databases, and other sources that have address information for use in QA/QC will greatly aid in resolving discrepancies by cross auditing multiple datasets.

Process Diagram

Each component of Figure 21 is a closed loop (Test → Correct → Test) that will iterate until the data meets the specified requirements.

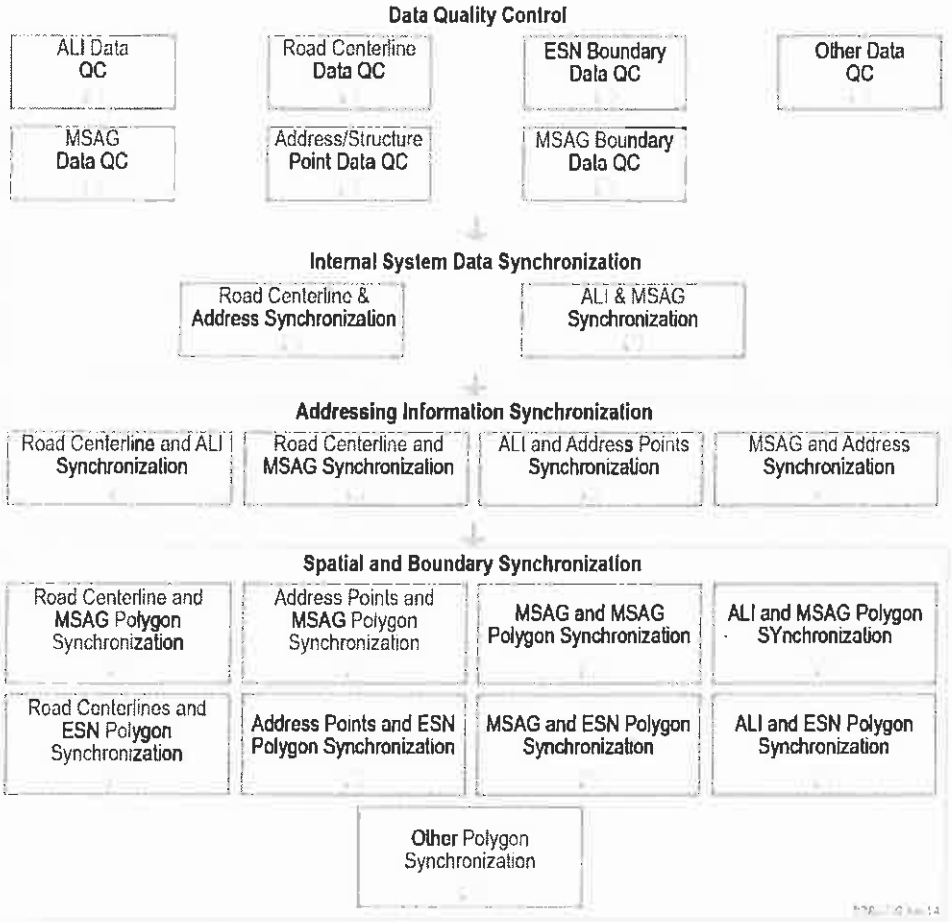


Figure 21. GIS Data Quality Control Process

The road centerline layer will be evaluated on naming, address range, and community fields. The naming fields will adhere to NENA 71-501, with conformance to USPS Publication No. 28 – Appendix C1. Special attention to punctuation and format of street spellings (1st vs. First) will be noted. State jurisdiction roadways and other primary carrier roadway naming will also be noted for future reference as they may require modification. The data must have clear and consistent street naming fields including a designated Left/Right area. The Street Name field must be populated for each record. If these fields are not correctly populated then some civic addresses may not be located, and the call will not be properly routed. The address ranges must correspond to the geometry of the polylines (polylines have a direction; therefore the ranges must match the "From" and "To" nodes of the geometry). This type of error will cause the location estimate for the civic address to be poorly estimated. It is possible that it will fall into the incorrect Service Boundary polygon and cause the call to be misrouted. The address ranges for segments with the same set of street naming fields cannot have overlapping address ranges. The left and right ranges for a segment cannot overlap (including overlapping parity). These errors can cause a prospective landline call to have multiple possible locations. Address range fields will not be in character format but rather be in numeric format with no special characters. Finally the community field will be analyzed to see if unique entries or misspellings exist which may be inconsistent for data comparisons. The road network will then be spatially analyzed for duplicate

geometry, invalid geometry, road direction (NENA 02-014 Section 4.3.5), and overpass/underpass situations where crossing geometry will not intersect.

Emergency Service Number (ESN) and MSAG Boundary Files

Since the PSAP, Fire, Law, and Emergency Medical Services will be derived from the ESN boundary data, it will be more efficient to use the ESN boundary layer for the synchronization. After this the derived layers can be created. However, we can do the procedures with the derived data if that is the preference. In this case, the references to the ESN polygons should be replaced and expanded by the derived layers. If the data transformation is isomorphic then the processes are equivalent.

The boundary files will be analyzed for spatial integrity identifying multi-polygons, gaps, and overlaps. These boundaries are then compared to the road centerlines for topology comparison. Unique boundary attributes indicate road topology changes so that the road centerlines can accurately reflect these attributes. The SIP URIs must be valid and working URIs for the ESInet call handling equipment.

Addresses Multi-Point Layer

Address points are an optional layer but are highly recommended to ensure accurate call location estimation in the NG9-1-1 environment. The following are the internal data consistency checks for this layer. Geocoding: In order to support call location determination, the street naming fields must pass the same requirements as the road centerlines. Uniqueness: If there is more than one record for a specific address and these records have different locations, then the location for the address is indeterminate.

E9-1-1 Data Quality Control

MSAG

The MSAG will be analyzed based on naming, address range and community fields. The naming fields will adhere to NENA 71-501 with conformance to USPS Publication No. 28 – Appendix C1 for naming consistency with the Road Centerline layer. Address range fields will not be in character format but rather be in numeric format with no special characters. The address range values must meet the minimum requirements for accurate geocoding. The ranges must be greater than zero. The high value must be greater than the low value. The values must match the parity field. The MSAG records with the same street name field values must not overlap with other records. The MSAG records must uniquely define a range of addresses. Emergency Service Number (ESN) fields will be analyzed for outliers and unique values. Finally the community field will be analyzed to identify whether it is represented by a city naming community style or community based on zip code.

ALI

The ALI data is not directly used in the NG9-1-1 environment, but will initially provide the source data for the LIF/LDB, and thus be used as the locations for call routing. It will be used to prepare the NG9-1-1 layers to ensure that the data reflects the legacy system for call routing determination (i.e., data synchronization). Any errors detected during the testing for internal data consistency will be reported for resolution. When possible, the GDIT team will provide recommendations for the proper resolution of specific errors. Additionally, there may be data inconsistencies that will need to be arbitrated by a central data authority. An example of this

would be two service boundaries that do not agree and may involve multiple local data authorities.

GIS, ALI, MSAG Data Synchronization

Once the data has been combined and has passed the data requirements for each layer, the next step will be to synchronize and test the various data layers for global consistency. The goal of the data synchronization process is to ensure that all the separate 9-1-1 layers are consistent with each other. In addition, the NG9-1-1 data must be augmented by and be in agreement with the legacy E9-1-1 system layers, the ALI and MSAG data. Table 5 illustrates the relationships that will be tested.

Table 5. GIS, ALI, and MSAG Data Synchronization Matrix

	Road Centerlines	Address Points	ALI	MSAG (Valid MSAG Addresses)	ESN Polygons	MSAG Polygons
Road Centerlines	X	Address to Centerlines	ALI to Centerlines	Valid MSAG Addresses to Centerlines	X	X
Address Points	X	X	ALI to Addresses	X	X	X
ALI	X	X	X	X	ESN Polygons Attributes to ALI	MSAG Polygons Attributes to ALI
MSAG	Road Centerlines to MSAG	Address Points to MSAG	ALI to MSAG	X	ESN Polygons Attributes to MSAG	MSAG Polygons Attributes to MSAG
ESN Polygons	Road Centerlines to ESN Polygons	Address Points to ESN Polygon	Geocoded ALI to ESN Polygons	Geocoded Valid MSAG Addresses to ESN Polygons	X	MSAG Polygons to MSAG Polygons
MSAG Polygons	Road Centerlines to MSAG Polygons	Address Points to MSAG Polygon	Geocoded ALI to MSAG Polygons	Geocoded Valid MSAG Addresses to MSAG Polygons	ESN Polygons to MSAG Polygons	X

The first step in the process will be to test the GIS addressing data consistency, road centerlines and addresses, the E9-1-1 addressing data consistency, ALI, and MSAG. The GIS and E9-1-1 data sets are most likely consistent since they have usually been maintained in a similar or central system. The process will be a closed loop of Quality Control testing and data corrections. The loop will iterate until the data meets the synchronization requirements set by MassGIS.

Road Centerlines and Address Points

If an address point layer is included then the first step will be to test the Road Centerline and Address Point layers for synchronization. For each address point there should be a unique road centerline record that matches the street name fields and whose address range contains that address point. There can be exceptions to this and each case will be examined. Once a unique match has been found, the spatial relationship between the address point and the corresponding road segment will be tested.

MSAG and ALI Synchronization

Each ALI record should match a unique MSAG record. The matching technique is very similar to the geocoding process, but since the MSAG is not spatial in nature, no location is estimated for the ALI record. If there is no matching record then the data must be corrected to bring it into synchronization. Multiple matches should not occur.

Addressing Information Synchronization

Once it has been confirmed that the GIS data is self-consistent and the E9-1-1 data is self-consistent, we will proceed with the first group of consistency tests between the two data sets. The process will again be a closed loop of testing and correction that will be iterated until the data meets the synchronization requirements.

Road Centerlines and ALI Records

Each ALI record should geocode to a unique road segment, in other words there must a unique road segment with matching street name fields that contains the house number of the ALI record. If there is no matching record then the data must be corrected to bring it into synchronization. Multiple matches should not occur.

Road Centerlines and MSAG Records

The MSAG records will be converted into a set of valid MSAG addresses. For example, an MSAG record for N,Main,St,Madison,100,200,B (N Main St Madison from 100 to 200 all integers) will be converted to a list of addresses 100 N Main St Madison, 101 N Main St Madison, ... , 200 N Main St Madison. Each valid MSAG address should have a unique geocoding match in the Road Centerlines data. If the Road Centerlines data has passed the internal check concerning overlaps, no multiple matches should exist. This leaves two outcomes: no matches and one match. The valid MSAG address records with no matches need to be reviewed and the appropriate correction applied.

ALI and Address Points Synchronization

Each ALI record should match to a unique Address Point record. If there is no matching record, the data must be corrected to bring it into synchronization. Multiple matches can occur due to the non-standard encoding of extra address information (Lot 52, Suite 101, etc.) in the ALI data.

MSAG and Address Points Synchronization

Each Address Point should match a unique MSAG record. If there is no matching record then the data must be corrected to bring it into synchronization. The matching technique is very similar to the geocoding process, but since the MSAG is not spatial, no location is estimated for the Address Point record. If there is no matching record then the data must be corrected to bring it into synchronization. Multiple matches should not occur because the MSAG data has passed internal consistency tests.

Synchronization to the MSAG and ESN

At this point, we have synchronized the GIS and E9-1-1 addressing data. We are now prepared for spatial testing and synchronization to the ESN and MSAG polygons. Each set of data that contains ESN and/or MSAG information will be spatially located. It will then be compared to the attributes for the polygon it falls into. In the case of a location that occurs exactly on a boundary of the polygon layer, the test will be considered indeterminate and will be reported.

Geocoded ALI and ESN Polygons

This test will verify that the NG9-1-1 data will return the same result for call routing as the original ALI record. Each ALI record will be geocoded to the Road Centerlines (and Address Points if included). The generated location will be compared to the ESN Polygons in order to determine which polygon contains it. The call routing information from this ESN polygon is compared to the call routing information in the ALI record. If these are different then it is classified as a mismatch, otherwise it is considered a consistent match.

Geocoded MSAG Valid Addresses and ESN Polygons

This test will verify that the NG9-1-1 data will return the same result for service determination as the original MSAG record. MSAG records will be converted into valid MSAG Addresses as outlined above and the valid MSAG addresses will be geocoded to the NG9-1-1 data (Road Centerlines and optionally Address Points). The generated location will be compared to the ESN polygons to determine which polygon contains it. The service information from the ESN polygon is compared to the service information in the valid MSAG address record. If these are different then it is classified as a mismatch otherwise it is considered a consistent match.

MSAG Polygons Synchronization

The two processes above will be repeated using the MSAG polygons as the target synchronization layer.

Data Extract, Transform, and Load Routines

Data Load NXG provides a framework to transform GIS data and a mechanism to load it into the DDTi Data Manager NXG system. The GDIT team will work with MassGIS to develop an appropriate data extract mechanism and to define a corresponding configuration for Data Load NXG.

Ongoing Operations

GDIT's proposed solution provides the following capabilities in coordinating the mapping database between existing Commonwealth systems and the DDTi Data Manager NXG, supporting the ECRF/LVF, LIF, and LDB:

- Data Submission
  - Data editing will be done within the local GIS environment. The data that is being edited will reside on the local system. The data will be submitted periodically by the local entity to the Data Manager NXG system. The system will process the data for changes, apply basic QC checks and any necessary transformations, and incorporate updates into the core database. The QC results and reports will be distributed back to the local entity.
- Data Quality Control
  - Data Manager NXG includes a Quality Control (QC) process that runs continuously and evaluates updates in near-real-time as they are incorporated into the core database. The output of these checks is one or more (depending on the QC checks that are used) QC error layers in the Data Manager NXG system.

- Users can view QC error layers using the Data Manager NXG user interface, and the QC error layers can also be exported to file-based formats. Because user submission happens immediately, QC errors are visible in near-real-time. This immediate feedback mechanism promotes continuous improvement in the GIS editing environment.
- The QC checks can be assigned to several different classifications: geocoding, standards, internal consistencies, and external consistencies (if any). These checks include most of the tests that were used during the data quality control and synchronization phases as previously described.

- Data Distribution
  - The data distribution function transforms, formats, and exports the data from the core database into files or other databases based on the client's needs. The publishing of the data can be restricted based upon errors detected during the QC process. Individual QCs are assigned to a customizable severity level, and individual thresholds can be configured for each severity level and GIS layer. These thresholds can be based on either the absolute count of errors or the relative rate of errors in the layer. If any of the QC error thresholds are violated, the publish process will be blocked. It is also possible for an administrator to configure a given publishing task to ignore the QC error thresholds, if needed.
  - The data distribution tasks can be initiated on demand, scheduled as a one-time publish, scheduled as a reoccurring publish, or can be triggered automatically by any changes following the completion of QC checks.
  - A database layer can be setup to be published to multiple user-defined export files. Each one of these exports can be customized in a limited way. The specific fields to export can be designated, and the output field name and format can be configured.

- Administrative Control
  - Administrators can configure quality control and data publishing from a web-based interface. Administrators can also control users, permissions, and display options.
  - In addition to standard health and monitoring of the NG9-1-1 functional elements, there are several outputs from the system that are useful for administrative purposes. Publishing failures (due to excessive QC errors, for example) will be configured to generate email notifications. Change report summaries and counts are available on a scheduled basis, and QC error summary counts and detailed counts by error type/description are available via the Data Manager NXG user interface.

Web-Based Map Updates

To help facilitate local data input and consolidation of the input for MassGIS, the GDIT team will setup a secure website that will allow local users to markup change requests that are spatially referenced to the GIS data. The GDIT team will consolidate all the change requests into a single database. There are options for the next step in the process, including:

- Unprocessed change requests can be exported to a specified format and distributed to MassGIS for updating the GIS data, which will then be used to update the ECRF databases.

- The GDIT team can convert the change requests into changes in the GIS record set. For example, these can be converted into Modify, Add, or Delete data changes. If the GDIT team has the latest copies of the MassGIS data, quality control can be performed on the changes. In addition, a customized distribution filter can be set up using the quality control results. The changes that are classified as passing the quality control can be exported and distributed to MassGIS. MassGIS can then update the GIS data and consequently publish to the ECRF. The changes that are classified as failing the quality control can be sent back to the user for the necessary corrections.

Regardless of the option chosen, the GDIT team will maintain a database of all historical changes, the state of the change request, the user that submitted the change request, and when it was submitted. This will facilitate any change rollbacks or change auditing that may need to be performed.

8.7. NEXT GENERATION 9-1-1 ARCHITECTURE

GDIT will comply with the RFR specification.

Detailed Solution Design and Technical Documents

The contractor shall, within sixty (60) days following contract award, submit to the State 911 Department for approval detailed solution design and technical documents that address, at a minimum, hardware, servers, logical, and software diagrams and specifications, customization and application design.

The GDIT team will submit a detailed solution design and technical documents that will include at a minimum hardware, servers, and logical and software diagrams and specifications for review and approval by the State 911 Department for the Commonwealth of Massachusetts.

Future-Proofing

The system shall be designed to future-proof the Commonwealth against the requirement for a 'forklift' upgrade of system components at any time during the life of the contract. Therefore, the system shall be designed to have the ability to accept new payload types without the need to replace the applications or appliances or CPE and the system shall be maintained in its entirety for the initial contract duration (five (5) years) without the need to replace or upgrade the applications or appliances or CPE.

GDIT is a vendor agnostic Systems Integrator (SI) that designs, implements, and operates best-of-breed communications technology and networks to meet our clients identified considerations, including the ability to meet future technology demands. A core tenet of GDIT's proposed solution for the Commonwealth is to leverage all defined NENA standards as the basis for all considerations, such that we support the existing and anticipated future NG9-1-1 construct. Understanding that NENA standards both continue to evolve and do not provide comprehensive definition of all aspects of the systemic solution, GDIT leverages over 40 years as a network technology SI, and deep experience in high-security, complex, and mission-critical network applications to augment our solution with highly established industry best practices and standards. We also leverage our 20 years of experience in deploying legacy 9-1-1 systems and our industry leadership in emerging technologies, including Unified Communications (UC), IP

Multimedia Subsystems (IMS), cloud computing, and mobility to further consider the direction of technology.

GDIT's proposed solution establishes NENA NG9-1-1 standards as the overriding solution construct, with the critical overlay of supporting standards as defined by the Commonwealth in Sections 8.2.1, 8.2.2, and 8.4.2 of the RFR. GDIT also leverages our extensive experience in deploying and maintaining mission-critical, high-reliability voice, data center, and public safety networks to ensure maximum flexibility in supporting new, evolving payloads, capabilities, and practices.

GDIT maintains close coordination with our partners to ensure all systems meet evolving standards on an end-to-end basis. The detailed solution design will include "future-proof" considerations such that the system components and overall solution will be able to accept new payload types and service mechanisms without the need to "forklift" system components during the initial contract duration period (five years). Such future service considerations include text messaging, video, Customer Information Database (CIDB), Policy Routing Function (PRF), and support for a public Location Information Service (LIS). Software updates and patches may be required during the initial contract duration period to comply with evolving NENA standards.

As outlined in greater detail in our response, GDIT's proposed solution meets all existing services demands, types, and capacities, with every primary ESInet system supporting over 100% of the Commonwealth's demands in each data center. With few exceptions, the increases in capacity for primary systems are supported through the increase of software licenses only and will not require additional hardware resources until over 200% of capacity is required. Where growth in resources is needed, all growth is incremental, without disruption to operational services.

Scalability and Expandability

The system shall be designed to be expandable, with the capability for expansion on an incremental basis, not a wholesale replacement of major platform(s). All subsequent system expansions and/or upgrades shall be backward compatible with components proposed in the response.

Bidders shall describe the scalability and expandability, indicating the related costs of the system in terms of processors, main computer memory, disk drives, peripheral devices, and connectivity of all CPE at the PSAPs and applications and appliances at the data centers as well as any other equipment.

Bidders shall state the expansion capability of the system equipment, describing the overall system capacities.

The system shall meet current needs as well as Next Generation 911/ESInet connectivity in order to meet anticipated future growth and changes to payload. The system shall be installed with adequate processor and hardware capacity to meet this demand.

Commensurate with GDIT's "best-of-breed" approach, we have aligned the NG9-1-1 core-competency leaders to bring the Commonwealth the most pure form of i3 collaboration as a single converged solution. This unified application experience allows for centralization of services within redundant data centers, cohabitation of applications and appliances using virtualization and blade servers for efficient use of power and space, and application scalability and redundancy at each PSAP, providing the Commonwealth the NG9-1-1 solution it can trust. These services and applications, provided by industry leaders in NENA standards, follow the framework of i3 and allow GDIT to provide the Commonwealth with the solution that delivers NG9-1-1 to provide communication management now and into the future.

GDIT's proposed solution for NG9-1-1 has been designed to deliver 100% of existing services demand in a high-availability configuration (hardware and software) within each data center, with failover redundancy between data centers. Additional capacity on these systems is achieved through the addition of software licenses at various points in the growth curve, with the ability to add hardware resources incrementally, without disruption to operational services. Capacity and expandability of all primary solution components are as follows:

- **Emergency Call Routing Function and Location Validation Function (ECRF/LVF):** The operational capacity of the ECRF/LVF is measured in queries per second, which is critically influenced by several factors associated with an individual call, including location by reference and the complexity of the map polygon that defines the service area. Depending on the call model, the ECRF/LVF can accommodate between 400 and 2,000 new 9-1-1 calls per second, roughly equating to between 1.5M to 7.2M calls in a given hour.

- **Location Database (Private ALI):** Four LDB virtual machines are deployed for Massachusetts, providing the HELD query interface. Each VM instance can handle approximately 1,000 queries per second. This means the system can handle 4,000 queries per second total with all servers online. These queries are initiated for each new 9-1-1 call, or a location rebid/dereference. Theoretically, the system can handle up to 4,000 new 9-1-1 calls every second

- **Emergency Services Routing Proxy ESRP):** Two ESRP i3 Evolution servers will be deployed in each data center as high-availability pairs. Each of the four servers will support approximately 120% of total services demands, and each can be queried independently. Each server supports (approximately) 300 call setups per minute, allowing 200ms per query.

- **Customer Premises Equipment (CPE)**: All software, licenses, and hardware required to support the simultaneous use of 1,000 (~120%) call taker positions is provided in each data center. Local (PSAP) systems are not required for CPE operation, other than the operator workstation and desired apparatus (printer, phone, etc.). Furthermore, the CPE can support over 400% of service queues (on hold), allowing each call taker to manage approximately five service requests simultaneously. Growth in the CPE is accomplished through the incremental addition of software and hardware, without disruption to the operational environment.

- **Border Control Function (BCF):** The BCF is a purpose-built appliance capable of supporting over 8,000 simultaneous sessions. GDIT's proposed solution provides licenses to support 1,000 (approximately 120%) of all call taker positions and services across all PSAP and training locations simultaneously. Growth is accomplished through the addition of software licenses.

- **WAN (edge) routers:** All routers specified are capable of supporting greater than 200% the initial configured capacity, without any change in software, hardware, or licenses.

- **Legacy Gateways:** GDIT's proposed solution includes legacy gateways as a component of the transitional configuration, allowing interface between the legacy carrier

environment and the NG9-1-1 environment. The Location and Network Interface Function (LIF/NIF) components of the legacy gateways are provided to support 120% of the initial services demands, with the ability to grow to 200% through the addition of software licenses (only). The Protocol Interworking Function (PIF) component of the legacy gateway are hardware based, and GDIT's proposed solution includes PIF capacity to support 100% of all identified carrier TDM interfaces. Growth of the PIF functions is achieved through incremental addition of appliances. As transitional components of the NG9-1-1 architecture, however, legacy gateways (LIF/NIF/PIF) will decline as carriers agree and enable SIP trunks between networks. Investment in excess capacity for gateways is identified as stranded investment and should be minimized wherever possible.

- **Access Loop Bandwidth:** Access loop (last mile) bandwidth connections to each site are specifically provided to meet required service and quality requirements based on worst-case calculations. GDIT identifies a minimum of 500k required per call taker position in order to support two simultaneous calls and mapping (Section 8.3.2.1, PSAP Network Bandwidth). GDIT's proposed solution provides a minimum of 750 MB per call taker position (primary, secondary, training, and limited secondary) to support additional future service types and growth. Every site will have a minimum of a 1.5MB connection.

- **Core WAN Bandwidth:** GDIT's proposed solution for Core network bandwidth supports 100% of aggregate bandwidth demand to all PSAP locations, with available spare capacity of a minimum of 200% of aggregate capacity. Further spare capacity and/or capacity expansion can be provided upon notice from the Commonwealth.

- **Storage:** Mirrored storage capacity of 14 TB is provided in each data center utilizing the EMC VNX5200 SAN, providing estimated capacity to support all expected storage demands for over six years. The storage systems can be incrementally increased through the addition of hardware without any impact on the operations of the storage systems or to services. GDIT's proposed storage network architecture includes EMC's RecoverPoint at each data center for data replication between VNX5200 storage arrays. RecoverPoint adds continuity of operations for the storage arrays in case of failure at the primary data center location, providing another layer of protection for the mission-critical data and applications in the Commonwealth's NG9-1-1 network.

Imaging Computers and Servers

The contractor shall deploy a mechanism to efficiently image computers and servers to minimize downtime and to ensure standard builds for computer systems.

GDIT's network management practices will include an imaging methodology that will allow for restoration of systems applications and operating systems, such that individual servers will not need to be manually rebuilt. The applications defined for this purpose will include the EMC file management system within the SAN and, where needed, imaging applications to include Windows Deployment Services (WDS) and EMC's Networker. The Networker application provides backup/recovery of files, applications, and complete physical or virtual servers. It facilitates creation of image-based snapshots of the entire system, inclusive of operating system, applications, configuration, and data. System images can be recovered to the same or dissimilar hardware. The combination of WDS and Networker will provide superior unified backup and recovery capability for the NG9-1-1 architecture. Additionally, GDIT will define scheduled

backup of all configuration files that will be necessary for bringing a newly imaged system to operational readiness, including which imaging application will be utilized. All backup and imaging information will reside in the storage systems.

GDIT's proposed storage network architecture includes EMC's RecoverPoint at each data center for data replication between VNX5200 storage arrays. RecoverPoint adds continuity of operations for the storage arrays in case of failure at the primary data center location, providing another layer of protection for the mission-critical data and applications in the Commonwealth's NG9-1-1 network.

Virtualization and Blade Technology

The contractor shall deploy virtualization and blade technology, where applicable, to improve efficiency, management, reliability and reduce server sprawl. The servers shall have hot swap RAID hard drives, redundant hot swap power supplies (with two (2) separate electrical inputs) or power sources depending on architecture. The servers may utilize clustering and other high availability technology to maximize system uptime. Bidders shall describe in detail the proposed RAID.

GDIT proposes a federated, multi-vendor solution, and we have worked with our partners to maximize the co-residence of systems on shared hardware platforms where possible to maximize performance, cost reduction, and environmental savings. Due to the mission-critical nature of systems, we have pursued a very conservative approach in this regard to fully maintain the redundancy and availability model, and to eliminate any potential for negative systems interaction. We have standardized on VMWare. Our solution also includes the use of blade servers to improve systems density and reduce power and space usage.

Server hard drive configurations at each data center are configured as RAID 1 with hard drives appropriately sized for the demands of the hosted application and/or database. RAID 1 meets the availability and redundancy requirements of the particular functional element. The proposed EMC VNX5200 storage array at each data center is configured as RAID 5, due to the amount of storage space needed (14TB).

Display Legacy ALI

The CPE shall display legacy ALI in a standard form, as specified by the State 911 Department, and shall be capable of exporting the legacy ASCII format out to the CAD interface port via serial and ultimately Ethernet. A sample of the current standard ALI screen is attached as Attachment J- ALI Format. The contractor shall provide an interface to an upgraded format at such time as an upgrade in location information (to Extensible Markup Language (XML) or otherwise) is published and approved for general use, as determined by the State 911 Department.

GDIT carefully evaluated multiple CPE solutions and selected the Emergency CallWorks CallStation CPE platform, which can accept Automated Location Information (ALI) in virtually any format over a variety of different link types. The system supports an unlimited number of ALI interfaces and can support multiple local and remote databases simultaneously using advanced ALI steering capabilities. The system includes a fully configurable ALI test parser that can recognize and break apart any ALI message format into individual data fields. The system then stores and displays the fields individually. This allows the individual pieces of data within the ALI message to be displayed to call takers in a customizable and consistent format and location, with associated labels. Further, text parsing allows new information to be added to the presentation of information, supporting the expansion of the ALI data set due to the evolving set of caller methodologies, including wireless and VoIP. Using this parsing, GDIT can ensure that

ALI information can be presented to call takers in the format identified in RFR Attachment J. CallStation currently supports ALI in XML format as part of a NENA i3 call delivery.

The CallStation solution includes a modular, templated, event-based system for outputting data to third-party systems, including CAD, mapping, and logging recorders. CallStation leverages the collection of individual ALI data fields from the parsed ALI message to facilitate reconstruction and output in any format imaginable. Customized templates can be configured to specify the selection and location of all fields. This includes the ability to support an unlimited number of different output formats as well as flexible position identifier re-mapping. A different template can be configured for each physical output interface, with no limit to the number of interfaces. At the remote side, data is either delivered as IP (i.e., RFC 2217) or can be converted to serial (i.e., RS-232). GDIT's solution includes an IP-enabled serial conversion device at every PSAP.

Security Protocols and Interfaces

Bidders shall describe, in detail, the security protocols and interfaces. If additional hardware (firewall, etc.) is required, this shall be included in the base system, not priced as an option.

The value, benefits, and capabilities of IP-based NG9-1-1 architecture are undeniable, but they also introduce new and significant burdens on assuring the integrity of the network and the privacy and assurance of information. These security considerations grow exponentially as network boundaries expand and as network access becomes more ubiquitous. GDIT's information security approach is built upon our extensive experience deploying and defending mission-critical information networks for federal and DoD customers. We are committed to a risk-based approach to mitigating threats to NG9-1-1 services and information guided by NENA 75-001 and 75-002, and leveraging best practices developed in other mission-critical environments.

A defensible network is one that provides visible and known points of entry (demarcation), thereby removing uncontrolled avenues of attack. Policy-based traffic controls can be placed at these boundaries to manage the flow of traffic by type, source/destination, privilege, and function, and traffic can be subject to protective treatments, such as separation and encryption. The components of the defensible network are configured and maintained in accordance with a standard baseline, as stated in NENA 75-001 for security of NG9-1-1 networks, to ensure that the prescribed security mechanisms, traffic configurations, and control points provide information assurance.

Where traffic management and control is critical to protecting the boundaries, a defense-in-depth approach must also consider internal threats and some level of threat penetration. As such, monitoring and vulnerability scanning become critical to identify, track, limit, and remediate threats. Such monitoring is highly similar in data flows and capabilities to network management monitoring, leveraging reporting from systems and inspection of packets to make determinations. Therefore, security-based tools operate in parallel to network management–based tools using highly coordinated tools and overall network design to ensure appropriate performance.

Security management is critically linked to network management, with the notable difference being the purposes of analyzing information and a (very) few differences in the tools and mechanisms used to collect and present information to administrators. As such, much of this discussion merges both network and security management constructs. The following is a partial

list of capabilities, mechanisms, and considerations that are key enablers of GDIT's proposed baseline solution (not priced as an option) in achieving the network and security management construct in compliance with NENA standards:

- **Border Control Function** – BCF is a required component of the ESInet architecture and serves as a dynamic firewall allowing voice services paths to be created and closed upon demand. In addition to ingress and egress protection at the data centers, the GDIT solution also places a BCF at each PSAP to offer an incremental level of protection beyond NENA standards.

- **Edge Router/Firewalls** – Each and every edge router will manage all ingress and egress traffic to each site as critical enabler of both the QoS mechanism and for network security. Each router is licensed to include a security bundle, including intrusion detection, encryption (IP Security (IPsec), Transport Layer Security (TLS), Secure Real-time Transport Protocol (SRTP), VPN (Generic Routing Encapsulation (GRE), and stateful firewall. Additionally, these devices are critical in managing QoS to all traffic by leveraging prescribed traffic engineering, including Differentiated Services Code Point (DSCP), VLAN separation, and traffic monitoring.

- **Central Policy Enforcement Point (PEP)** – GDIT's proposed solution leverages edge routers as PEPs at each location for traffic entering and leaving the ESInet WAN. All traffic entering from the WAN is treated as untrusted. With the dominant traffic flow occurring between the data center and the individual PSAPs, centralized firewalls, and Intrusion Detection System (IDS) are also provided to increase capacity and protection on traffic entering and leaving the data center to limit propagation of treats.

- **Intrusion Detection System (IDS)** – This is an advanced security function that allows traffic to be inspected at network boundaries for known viruses, policies, and malicious attack profiles. GDIT's solution provides IDS as an integrated component of all edge routers at every site. Additionally, each data center will deploy a centralized IDS.

- **Logging** – Separate from the NG9-1-1 event logging, each system in GDIT's solution is configured to create and send logs on all system operations, including administrative access and changes, capacity reports, and system health. These logs are collected, indexed, and stored as critical pieces of input for both security and network management. Logs include SYSLOG, WMI, and various text.

- **Encryption** – Data encryption utilizing IPsec is provided on all IP services leaving the PSAP or data center in compliance with NENA standards, such that no information is decipherable should it be intercepted. Encryption is supported with anticipated use of L3 Virtual Private Network (VPN) tunnels to increase privacy and provide critical separation of traffic by types across the IP WAN.

- **Messaging** – SNMPv3 is defined by NENA as the necessary protocol for management messaging. While not all components of GDIT's solution presently support SNMPv3, each component has a roadmap to offer this capability in the near future. Until then, SNMPv1 or 2c, WMI, or other messaging protocols will be used. To support the privacy of these messages (intended by SNMPv3), traffic will be encrypted at the data layer.

- **Storage** – This is a critical component for network and security management and is a historical archive for event logging recording. Centralized storage offers a vastly superior ability to efficiently manage and use historical information, including backup, aging, and retrieval. GDIT's proposed solution places approximately 14 TB of mirrored storage at each data center, which is expected to support over five years of operations without any aging of files.

- **Authentication and Authorization** – GDIT's proposed solution includes a policy-based Active Directory (AD) environment to provide centralized Authentication, Authorization, and Accounting (AAA) for managing access to the network for all privileged users, including administrators, supervisors, and call takers. GDIT's proposed solution employs a redundant, centralized, and role-based authentication policy engine to manage access of all users, from all locations, to all (capable) devices. The solution will leverage a Microsoft AD group management policy, maintained at (redundant) master domain controllers at the data centers. The AD will authenticate users with their associated role-based mapping on Terminal Access Controller Access-Control System (TACACS), Remote Authentication Dial In User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP) enabled systems. Systems not capable of LDAP or RADIUS will be maintained independent of the AD structure.

- **Vulnerability Management** – The network is subject to threats from external and internal penetration, or from erroneous internal behavior that typically results in changes in network configurations. Vulnerability scanning performs analysis of the network to identify unauthorized changes and/or security policy violations and activity that may indicate either a potential threat or an active threat. Vulnerability management is being performed by the Tenable Nessus system, residing in each data center.

- **Security Incident and Event Management (SIEM)** – SIEM functionality will be provided by GDIT in a composite solution leveraging the AlienVault, SPLUNK, and Cisco Security Manger systems to collect, index, and report on information provided by all systems through logging and messaging. GDIT's experience is that this composite approach provides exceptional visibility and performance at a reasonable cost. A future, higher-level (e.g., aggregated) SIEM may be considered if and when the Commonwealth believes the level of incident and event reporting may warrant the additional cost, although this is not expected to be warranted.

- **Network Services** – The need for IP network services is a critical enabler of services reliability and quality, which also has security and network management considerations. All network services to ensure industry best practices and NENA compliance are included in GDIT's proposed solution, including:

  — Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are provided in a redundant configuration from the domain controllers located within each data center.

  — IP Address Management (IPAM) is supported through the SolarWinds OSS platform.

— Network Time Protocol (NTP) is provided through redundant, NENA-compliant servers also located at each data center.

- **Update and Download Server/Solution** – Most, if not all applications, devices, and services within the NG9-1-1 environment require periodic and/or recurring updates. Some of these services, such as McAfee AntiVirus and Windows Server OS, have particularly regular and/or time-sensitive update requirements, necessitating automated updates. Update and patch management solutions provide controlled, secure, managed, and timely updates to systems and services. This is accomplished using a highly controlled public connection, leveraging a DMZ and zone-based architecture.

- **Workstation Protection** – Each workstation will leverage anti-virus and firewall to minimize the introduction of malware to the ESInet. Each workstation will require authentication. Each workstation will be configured in collaboration with Commonwealth policy to allow and manage the introduction of removable drives and connectivity to outside networks.

- **Network Maintenance Tools** – Systems and solutions that are used to facilitate centralized management and interrogation into the accurate and intended flow of data across and between networks, with particular attention to information support SLA management to both the LAN and the WAN providers.

Section 8.4 (Network Security) provides additional details related to the overall proposed security solution.

Support for Future Potential Payloads

The State 911 Department intends to be able to handle, in addition to traditional voice calls, new and additional payload types in the future, potentially before national standards are fully adopted and when available from providers. The system architecture shall support all potential payloads without changing out the core logic or hardware. The response shall describe these functions and how they act to ensure compatibility with future call types.

GDIT's proposed NG9-1-1 solution includes i3 capabilities that support voice and text capabilities today. GDIT understands that standards for new service and payload types – including document transfer and multimedia delivery – are still evolving, and all of GDIT's technology partners in our proposed NG9-1-1 solution not only monitor evolving standards for multi-media services, but are also actively participating in the ongoing development of the standards.

Our technology partners have been participating in NG9-1-1 NENA Industry Collaboration Events (ICE) to provide standards-based compliance prior national standards being fully adopted, and our team has full understanding of the NENA standards development and evolving payload support status and progress.

In addition to preparing for and supporting future new payload standards, a core tenet of GDIT's multi-vendor technology approach is to rigorously leverage standard protocols and routing mechanisms. In doing so, GDIT's technology approach closely follows industry-leading applications that are pioneering highly analogous capabilities, including Unified Communications (UC), Cloud services, IP Multimedia Subsystem (IMS), and Web 2.0. As a result, GDIT believes our technology partners and approach provide both the awareness of

NENA technology trends specific for the public safety applications and the flexibility to leverage standard techniques in support early adopters. Presently, all routing ESInet components in the proposed architecture are working in advance of the SMS/MMS implementation leveraging Message Session Relay Protocol (MSRP) as the transport protocol. This support includes active participation in the ICE 6 event, demonstrating initial capabilities. It is expected that final standards and methodologies will be finalized in 2014, and that compliant implementation of the GDIT will be supported in 2015.

Network Bandwidth and Latency Tolerance Requirements per Position

Bidders shall describe the requirements of network bandwidth and latency tolerance requirements per position. Bidders shall also describe any additional data or networking equipment, not specifically addressed in this RFR, required at a PSAP and at data centers.

GDIT defines the minimum required bandwidth as 500k on a per-workstation basis using the following considerations:

- 110k per voice call
- 2 simultaneous calls
- 10% management traffic (~20k)
- 256k for mapping traffic

The addition of texting (SMS) will have negligible impact on these bandwidth requirements and, thus, texting is supported in these calculations. To accommodate some growth in future services, including an increase in call volume, an increase in number of call taking positions, and the addition of new payload types, and based on the relatively small incremental circuit costs, GDIT's proposal has priced in 750k per call taker position (at minimum). GDIT expects that the additional bandwidth will provide considerable flexibility to the Commonwealth for the growth in call taker positions and the incremental addition of some new services, including multimedia texting (MMS), document delivery, centralized applications (recording), and some video.

Bandwidth is a gross measurement, taking the total amount of data transferred in a given period of time as a rate, without taking into consideration the quality of the signal itself. Because signal degradation tends to occur as bandwidth reaches maximum capacity, we have specified the absolute minimum bandwidth we recommend to guarantee clear communications.

A holistic approach to QoS must include both packet performance criteria and traffic engineering. Packet performance criteria is defined by the Commonwealth in Section 8.3 of the RFR and will be met by GDIT, including packet loss (0.5%), Jitter (20ms). and (round trip) Delay (20ms). Our assessment is that the Commonwealth's criteria is very strict, and that industry best practices for end-to-end real-time services for packet loss jitter and (round trip) delay are 2%, 20ms, and 80ms, respectively.

Traffic engineering is a means of managing the prioritization of certain packets and provides a set of mechanisms and rules that reduce the potential for instantaneous traffic congestion. Where overall bandwidth may be many times greater than needed to support the maximum services, the instantaneous need for 'bursty' traffic many cause prioritization issues if appropriate mechanisms are not implemented. Common networking requirements that support end-to-end real-time services include:

- Real-time traffic should comprise no more than 50% of total available bandwidth
- Put VoIP bearer and control traffic into a strict priority Low Latency Queuing (LLQ) with guaranteed bandwidth
- Real-time traffic should be configured with both L2 and L3 tags leveraging Type of Service (TOS) and Differentiated Services (Diffserv). Recommended Diffserv Point Codes (DSCP) values by payload type include:
  - (L3) DSCP Voice = 46
  - (L3) DSCP Video with Audio = EF45
  - (L3) DSCP Interactive Video = AF41
  - (L3) DSCP Streaming = 32

NENA standards define the enablement of a secure, resilient, and assured service ESInet WAN connectivity between all sites utilizing MPLS and/or Layer 3 VPN tunnels. Where both methodologies are supported by GDIT's solution, we believe an L3 VPN implementation and a combination of internal and external BGP offers operational simplicity and increased ability to locate faults and/or performance issues. This choice is further supported by the predominant traffic flow between the data centers and individual PSAPs, and less traffic between PSAPs. GDIT's proposed network topology is based upon VPN architecture used to encrypt all traffic between data centers and PSAPs. This network design was chosen for security, reliability, operational maintainability, and ease in troubleshooting. Figure 22 represents the routed connections across the ESInet WAN.

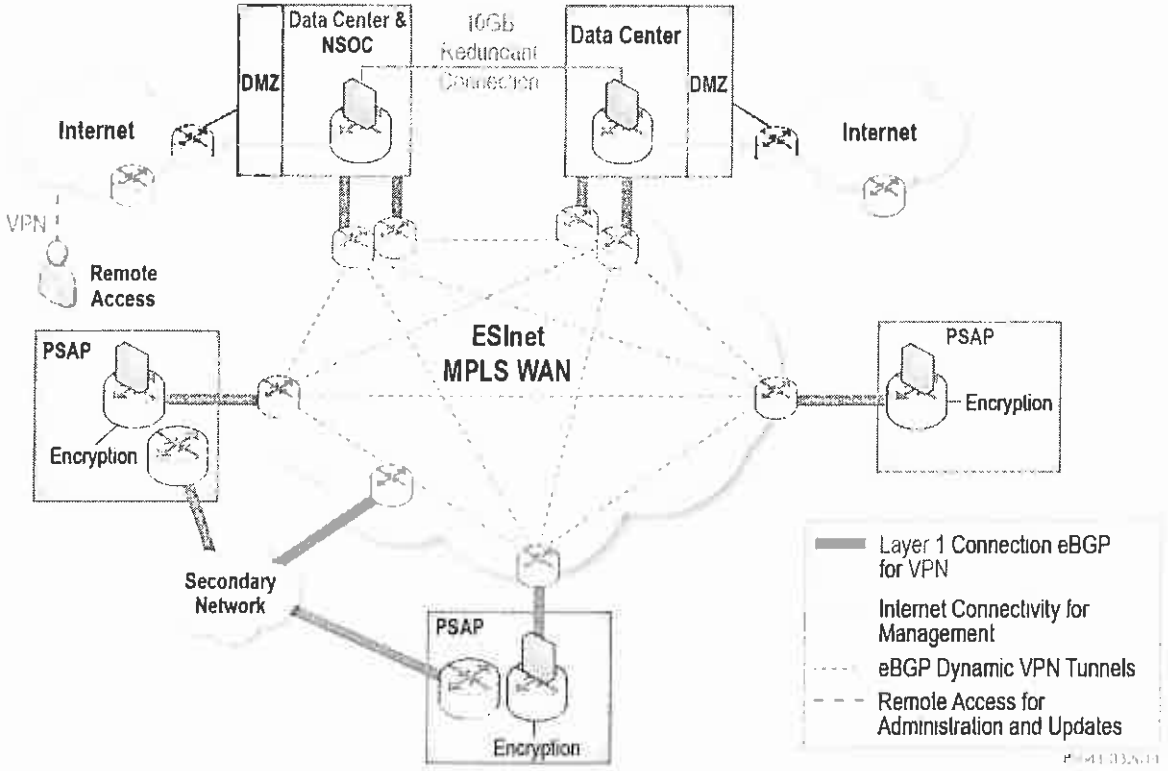


Figure 22. ESInet WAN Routing

GDIT provides individual PSAP models based (largely) on the size of each site and identified redundancy requirements. These models represent the data network connectivity between the ESInet WAN and internal ESInet LAN configuration within each PSAP. Critical to these models are the edge routers that serve to provide demarcation between administrative domains, providing policy enforcement for security, monitoring for QoS and SLA management, and redundancy of network connections. The following capabilities are provided in every remote service location (excluding the limited secondary):

- **Management Server:** Each management server includes a set of tools and functions that support the remote operation and management of the sites, including:
  - QoS probe that passively inspects and analyzes all session traffic, and provides the analysis of QoS and Call Detail Records (CDR) to the centralized server.
  - Local (read only) domain control to ensure systems authentication in the event of an ESInet failure.
- **Network Timing Server:** A master NTP server to ensure accurate and stand-alone timing to all systems.
- **Printer:** Network printer that will be addressable from each call taker position.
- **CAD Interface:** Network addressable IP to serial converter device that enables CAD spills to legacy systems with serial interfaces.

- **Voice Gateway:** An enabled feature of the Cisco router to provide an analog interface to local (existing) PSTN trunks for in/outbound administrative calling. With this capability, administrative calling is allowed even with a failure of all ESInet connections.

In the largest model (Figure 23), designed to support approximately 17–45 call taker positions, full redundancy of all networking systems is provided, in addition to the availability of primary, secondary, and tertiary ESInet connections. In this model, the (separately priced) option is provided to deploy local CPE to serve as a local call distribution among all positions. In this model, the local CPE would be redundant to the serving data center.

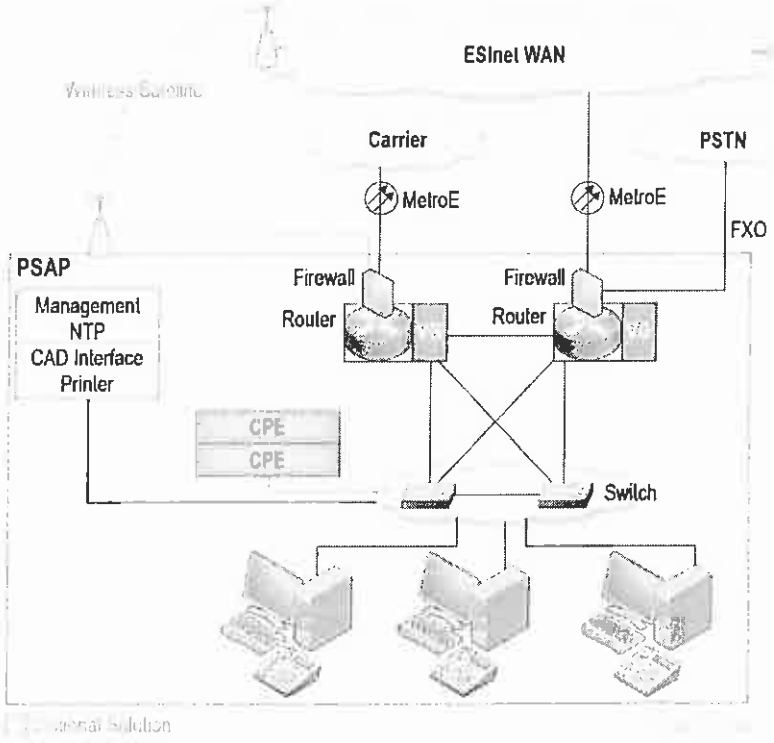


Figure 23. 17–45 Position PSAP Model

The second model (Figure 24) is similar to the largest model, but uses smaller routers (lower demand) to support 6 to 14 will be provided locally, although these options are fully supported.

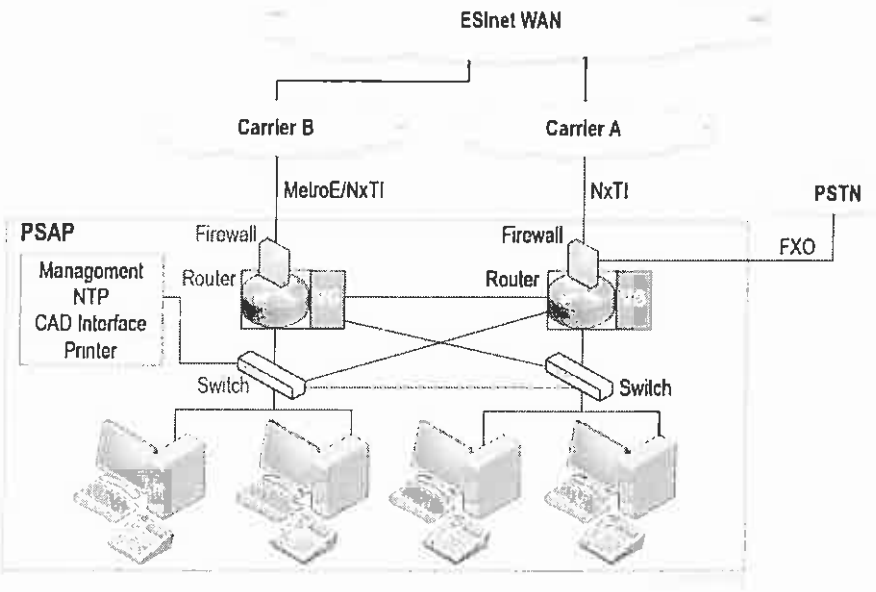


Figure 24. 6–14 Position PSAP Model

The smaller model (Figure 25) is intended to support 2 to 5 positions and offers redundant network connections and routers as an option.

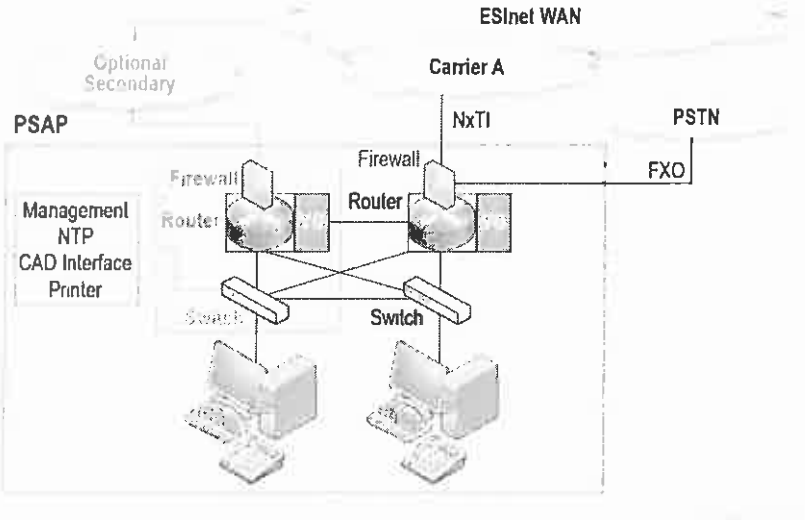


Figure 25. 2–5 Position PSAP Model

GDIT's solution includes all data and networking hardware, software, and licenses needed to ensure the PSAP NG9-1-1 is fully functional and integrated into the ESInet, and data center applications.

CPE Configured to Process the Payloads for Voice and Data

Bidders shall describe how the CPE and the applications and appliances are configured to process the payloads for voice and data. The system shall provide the minimum functionality as follows:

A. In the event of a failure of the active server, switchover to the second server shall be automatic and shall result in no loss of service;

B. The system shall have a non-blocking, fault tolerant switching fabric which is expandable;

C. Provide a robust architecture to limit dropping 911 payloads due to a hardware or other failure; and

D. Interfaces shall support detected tones, generate tones, and support audio conferencing.

The CPE shall be capable of supporting traffic to and from:

Other entities directly on the ESInet;

Legacy network gateways;

Legacy PSAP gateways; and

Other entities directly from their i3 networks.

The system shall incorporate VoIP technology. The system shall be accessible via Virtual Private Network, for virtual PSAP operations, online monitoring, system administration, and maintenance.

The contractor shall present a detailed architecture design for the system (as built), along with text description and annotated diagram(s). The descriptions and diagram(s) shall clearly identify interfaces and components functions.

The system shall be IPV6 capable.

Section 8.7.3 (Customer Premises Equipment) and Section 8.7.4 (Applications and Appliances) provide specific details on the proposed CPE. The proposed CPE, Emergency CallWorks' CallStation is a compliant NG9-1-1 CPE that fully integrates into the NG9-1-1 construct, supporting all defined interfaces and connectivity within the NG9-1-1 dataflow including support for SIP, HELD, and SIP-URI. Typical call flow in the transitional and planned final NG9-1-1 environment is shown in Figure 29 and Figure 30 (in Section 8.7.1), and include both the transitional environment utilizing legacy gateways and LDB, and the planned final environment.

CallStation is a VoIP softswitch, providing call processing and control leveraging all NENA standards and industry best practices to provide resilient, non-blocking call distribution over IP connections. As defined in the NENA architecture, legacy (TDM) inbound traffic is converted to IP within the PIF functions (gateways) before it enters the ESInet. Because the transitional environment is temporary, pending the native IP connections with the carriers, the PIFs are sized to terminate the full capacity of the Commonwealth's TDM trunks. It is expected that this number of trunks will decrease substantially through the efficiencies of aggregation, as described in greater detail in Section 8.7.1, Routing Requests.

GDIT's proposal has equipped and licensed CallStation to support 1,000 simultaneous calls at each data center, providing approximately 120% of total maximum capacity of available call taker positions. Physical resource and license capacity is provided during staging to allow testing to 200%. The proposed license and hardware configuration supports up to four (4) times this number of calls simultaneously being held in the CPE queue, allowing each and every call taker position to have multiple calls on hold while also serving the active calls. Additional capacity can be added incrementally to support growth in call taker positions without impact to the operational environment.

The CallStation platform provides a non-blocking, fault tolerant switching architecture that leverages two levels of redundancy to ensure no single point of failure at either the systems level

or the facility/network level. Within all/each data center, CallStation is deployed in a high-availability cluster, where each component within the critical call path is actively supported by two independent physical instances. The active machine in the cluster handles all server activity, and the standby machine is configured identically with a dedicated synchronization link. Failure of any active server is survived by the mated server without loss of any service capacity or capability. Each server cluster delivers 99.999% availability.

The second level of survivability provides a geo-diverse configuration across multiple data centers, each with a High-Availability (HA) configuration. Where single and many multiple failures are survived within a single data center (HA) cluster, catastrophic data center failure or network isolation will be survived through service-aware routing of traffic to the mated clusters at the alternate data center, termed a supercluster. In a supercluster, service configuration and awareness is synchronized across a dedicated 10G redundant network connection provided in the GDIT solution between data centers. Voice and data can be automatically re-routed within the system should a PSAP position or entire PSAP become unavailable. The processing and re-routing of voice and data payloads also occurs in the event of ring timeout, or when the PSAP's configured maximum number of calls waiting is exceeded. The proposed CPE system will also re-route calls if they have not been answered within a configurable amount of time and can also re-route based on a configurable number of calls that are already holding for answer. Illustrations of the two data center and three data center models are shown in Figure 26 and Figure 27.

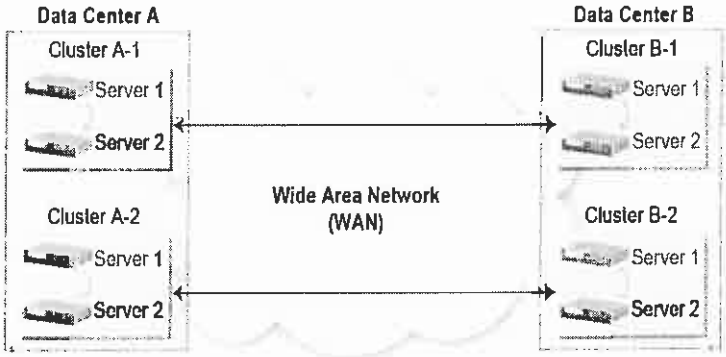


Figure 26. Two Data Center Model and Clustering of CPE between Data Centers

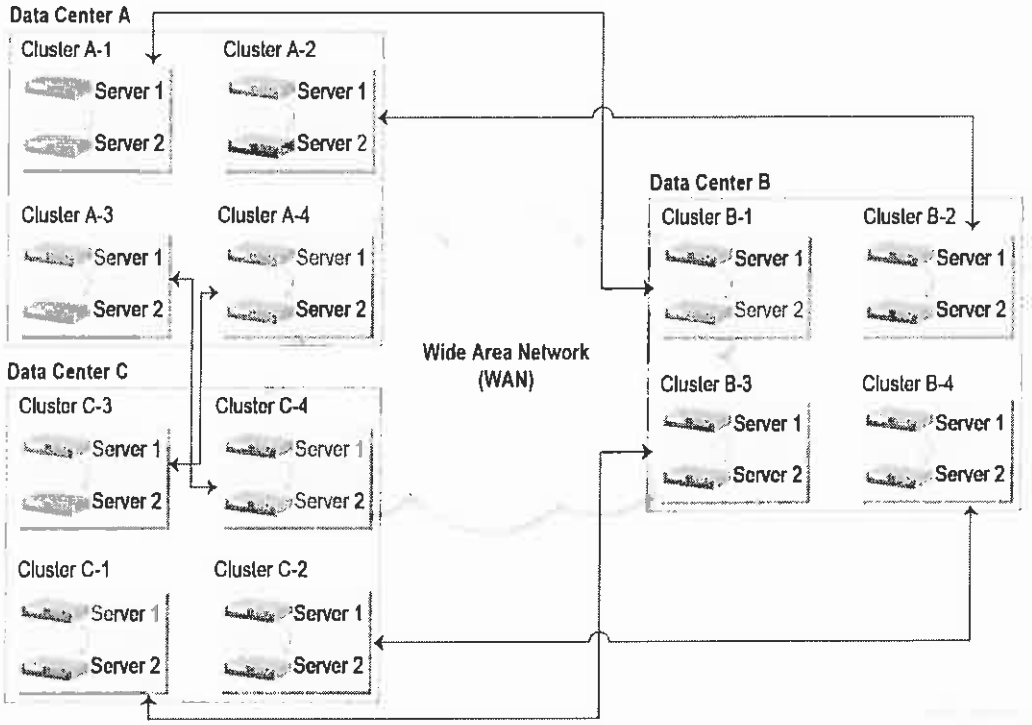


Figure 27. Three Data Center Model and Clustering between Data Centers

Unlike other CPE systems, GDIT's proposed routing solution checks the availability of the remote PSAP *each time a call is routed*; this alleviates the need to perform 'polling' and provides instant failback when the PSAP returns to availability. This method eliminates the average one-half polling period delay introduced by polling systems. All re-routing rules and thresholds are configurable on a per 'Dispatch Group' basis.

CallStation is a complete software-based solution employing a runtime services based software architecture that leverages independent software routines for performing identified functions (Figure 28). This provides critical separation of tasks and allows highly efficient management of physical resources. A key mechanism for achieving the HA clustering in CallStation is the Cluster Resource Manager (CRM) function provided on each server. The CRM actively monitors all key processes on the server, with the ability to stop and restart services as necessary. If there is a hardware failure or a critical service cannot be resurrected from failure, the CRM will automatically transfer all services to the alternate cluster node. This switchover happens within a few seconds and maintains service availability without any intervention by administrators and without requiring any adjustments by users.

CallStation supports detected tones, generates tones, supports audio conferences, and supports IP version 6 (IPv6).

As part of the detailed design deliverable that is due 60 days after contract award, GDIT will provide a detailed architecture design (as built) along with text descriptions and annotated diagrams that will clearly identify interfaces and component functions.

8.7.1. Routing Requests

The system shall have the ability to handle routing requests, including without limitation, default routing, rules based routing, and alternate routing, immediately by or upon the request of the State 911 Department. Bidders shall describe the functionalities for routing calls and shall describe the interfaces for routing calls. The process for routing requests shall be mutually agreed to by the parties.

The GDIT-proposed solution is NENA compliant and incorporates transitional elements to ensure a seamless interworking between existing carrier infrastructure and the NG9-1-1 architecture. As reflected in Figure 29, GDIT's proposed transition follows the NENA transition guidelines 77-501, fully accommodating all three legacy methodologies for connections to the services provider networks, including:

- Re-directing trunks presently between the selective router and the PSAP location to terminate at both data centers. This option can be least desirable as it leaves the selective router in place, and potentially reduces the interface trunk efficiency (analog CAMA and T1). This option may be used where carriers have significant difficulties in providing other termination options (listed below).

- Providing direct termination between the data centers and the individual carriers, and having the carrier direct emergency services traffic to the data centers rather than to the selective router. In this option, more efficient interconnect options are available, including SS7 and digital T1, and the selective router is no longer required.

- Direct SIP trunking between the data centers and each carrier. In this case, legacy gateways needed to terminate TDM trunks can be eliminated, and duplication of traffic to multiple and geographically diverse destinations (including a third data center) becomes practical. This construct is also the first step in achieving the NENA-specified methodology for achieving location collaboration between the carriers and the ESInet.

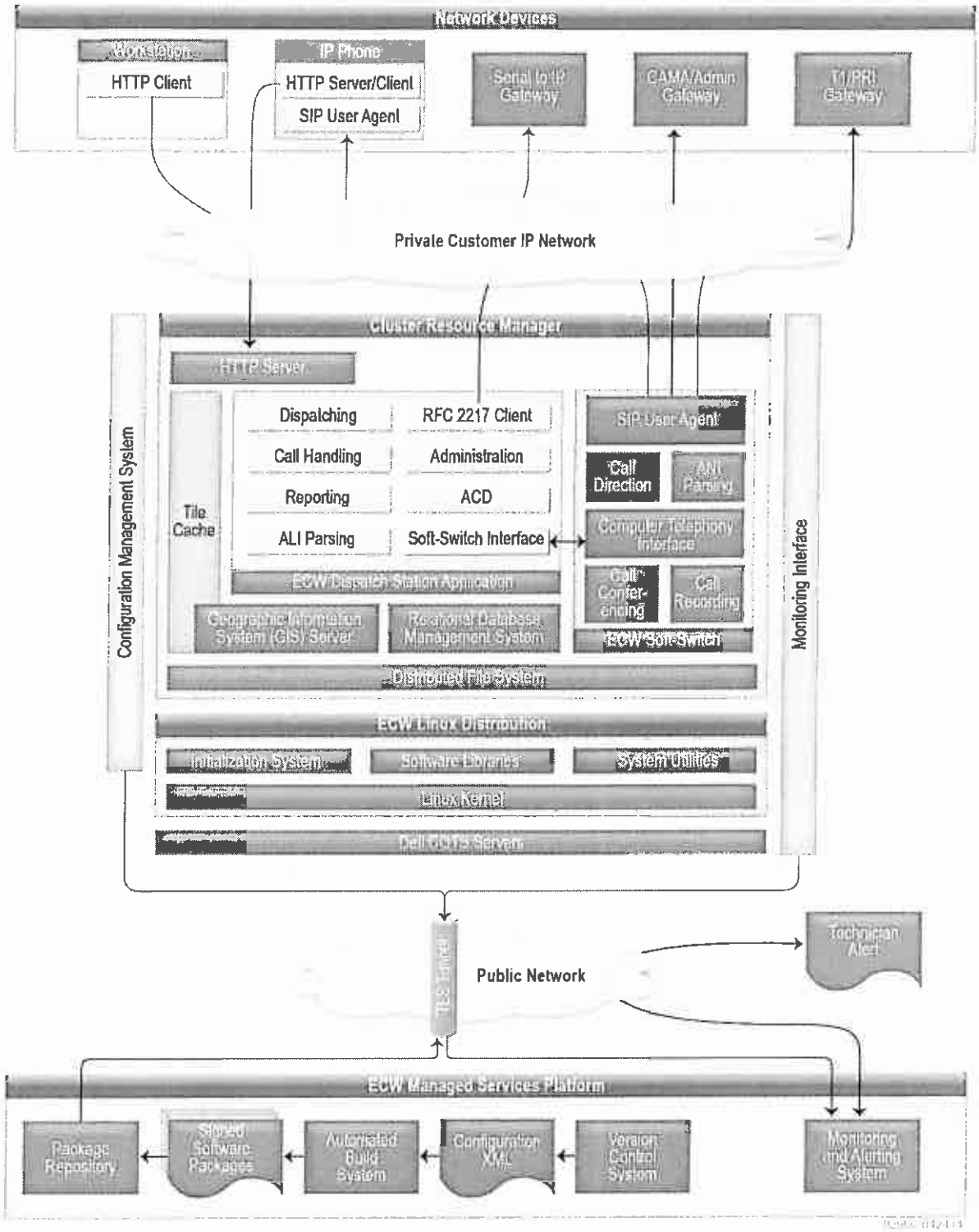


Figure 28. CallStation Software Architecture

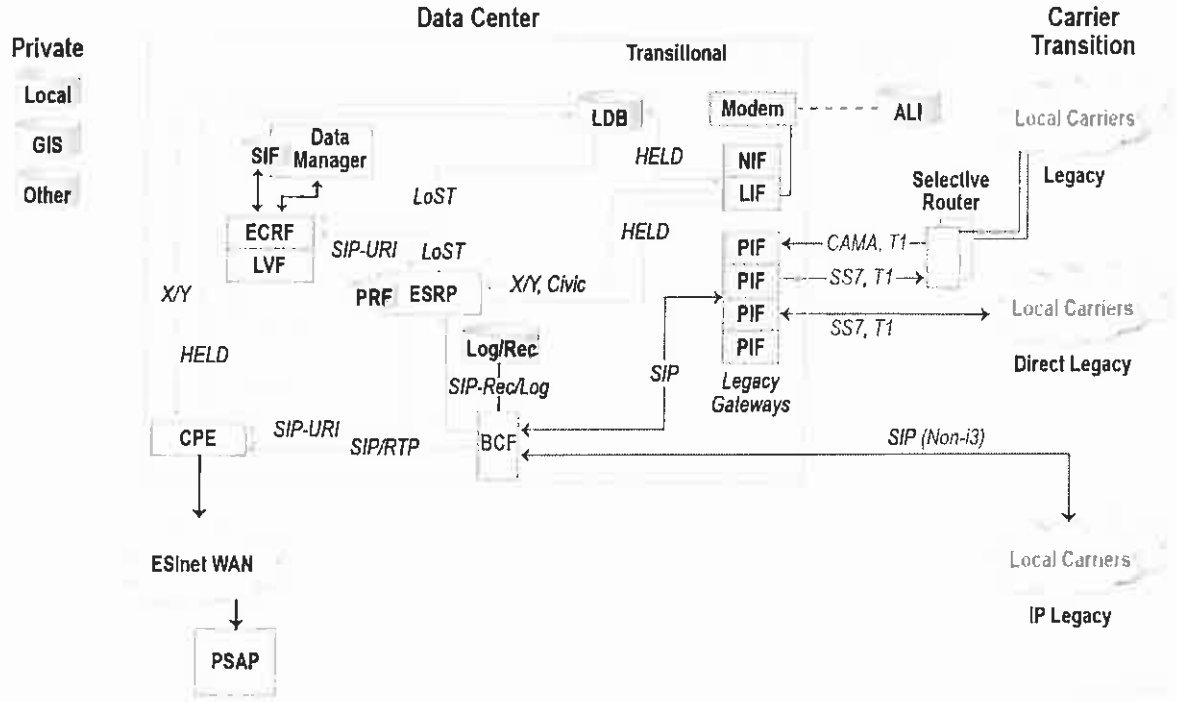


Figure 29. NG9-1-1 Architecture with Transitional Systems and Interfaces

Upon contract award, GDIT will work with the Commonwealth and together collaborate with carriers to identify and facilitate the most effective termination possible, and continue to maintain efforts to pursue the NENA-specified construct. Timing, regulatory constraints, and competitive pressures may dictate how each carrier reacts.

When TDM trunks are provided from a carrier to deliver 9-1-1 traffic to the ESInet, IP gateways – termed Proxy Interface Function (PIF) – serve to terminate the trunks, convert the traffic to NENA-compliant IP, and allow the traffic to enter the ESInet. The PIF is one of the three functional components of each legacy gateway, including the Legacy Network Gateway (LNG), Legacy Selective Router Gateway (LSRG), and Legacy PSAP Gateway (LPG). The two additional components of the legacy gateways are the Location Interface Function (LIF) and Network Interfaces Functions (NIF). These software functions are necessary in a transitional environment where location information in not provided by the carriers (through the LIS) and, therefore, requires a transitional construct for accessing and inserting location information (termed PIDF-LO). GDIT's proposed solution utilizes a Location Database (LDB) to serve as both ALI and LIS in the transitional environment.

GDIT is proposing the initial deployment of two data centers, and the optional deployment of a third data center, with each location capable of supporting the entire demands of the Commonwealth, Where the ESInet and WAN routing of NG9-1-1 services fully supports the three data center configuration, the connectivity of inbound 9-1-1 traffic from the carriers (e.g., ingress traffic) and how this traffic is provided to all data centers simultaneously become critical considerations. The question becomes how traffic is duplicated and distributed from each carrier to each data center, and what considerations will drive a carrier's agreement to pursue the various options, including regulatory drivers, competitive inclination, technology capabilities,

and revenue protection. Furthermore, because each carrier has differing drivers, because all carriers must be included in the initial architecture, and because each carrier offers a differing timeline for evolving their connections, all options must be considered valid and supported in the architecture initially.

During the legacy transition period (see Figure 29) some carriers are expected to initially connect ingress traffic using TDM trunks. Two options for TDM connections are valid:

- Redirecting traffic from the existing selective router pairs, and
- Providing direct connections to each carrier and bypassing the selective routers.

The least elegant, and possibly most expensive, option for TDM connectivity is to simply redirect existing traffic from the selective router (SR), from terminating at individual PSAPs, to terminating at each data center. In this scenario, the Incumbent Local Exchange Carrier (ILEC) will create new selective router routing translations, as if the PSAP has changed address. The data centers would need to equip IP gateways (PIF) capable of supporting analog trunks.

Many considerations exist with this scenario, including the fact that most, if not all, of these individual PSAP connections use single voice trunks (CAMA) and ALI/ANI circuits that are difficult and expensive and transport. Further, there is no known mechanism for duplicating TDM CAMA circuits. As this does not support survivability, the means for continuing to support traffic from all selective routers to all data centers is to convert the CAMA to IP either locally at the selective router or in near proximity. This conversion could be performed by the ILEC, or the ILEC would need to allow the placement (colocation) of IP/TDM gateways (PIFs). In this scenario, GDIT would locate the PIFs in the colocation space at or near the selective routers. GDIT's proposed solution does include PIF gateways. A variation of this 'legacy' methodology is to convert analog CAMA to T1/T3 at the selective router and provide protected transport to an outside colocation facility where gateways can be located. This alternative offers additional cost and complexity.

Agreements for pursuing either of these legacy alternatives are subject to negotiation with the incumbent and critical to timing considerations with regard to the Commonwealth's intended project schedule. GDIT's proposed solution includes the cost of the PIFs (regardless of placement location), and the required CLEC license from Windstream to perform colocation/termination of all trunks. GDIT assumes carriers will provide connectivity to our proposed PIF from the selective routers, pending connection agreements with the incumbent.

GDIT understands, however, that the Commonwealth intends to eliminate the selective routers and immediately pursue the interface option of directly connecting between each carrier and each data center (bypassing the selective router). When TDM connections are needed to connect directly to a carrier, SS7 connections will provide an automatic failover mechanism between the carrier and each data center. In this scenario, SS7-enabled gateways (PIF) will be deployed at each data center. In this model, GDIT assumes that each carrier has the responsibility for terminating SS7 trunks at each data center.

GDIT expects that all carriers will agree and facilitate direct carrier connectivity initially. Further, we believe from regulatory rulings that carriers are obligated to connect to the public safety demarcation at no cost to the Commonwealth, be it the selective router(s) or ESInet data center. However, timing is critical to the transition schedule, and certain carriers may have

network limitations, regulatory concerns, or competitive pressures that could delay their support. To reduce risk of meeting the Commonwealth's transition schedule, GDIT has included in our price, PIF capacity for terminating 100% of all traffic demands as TDM, and that 25% will be CAMA and 75% will be SS7.

TDM connectivity in either the legacy or direct legacy model represents complexity and costs. IP (SIP) connectivity between carriers and the data centers offers a direct path toward the NENA end state (Figure 63) and exceptional efficiencies in connectivity and greater flexibility in duplication to multiple destinations (data centers). In this scenario, distance of transport and duplication of traffic is readily available, making a highly geo-diverse (outside the Commonwealth) third data center both cost-effective and fully supported by inbound traffic. GDIT assumes that not all carriers will support direct IP connectivity initially. However, our proposed solution includes the systems, software, and licenses to support 100% of all ingress traffic as IP or TDM.

Upon award, GDIT will immediately engage with the Commonwealth and all carriers to facilitate and define the carrier connectivity methodology. With the Commonwealth's support and insistence, we strongly believe we can reduce or eliminate completely PSAP carrier connectivity circuit costs to the Commonwealth, including elimination of SR trunks, by establishing new, redundant connections directly to carriers and creation of the ESInet WAN.

IP traffic entering the ESInet is routed as specified in NENA standards utilizing the SIP traffic flow and the insertion of location information for routing to the appropriate call taker at the appropriate PSAP, and presenting the calling party information. While the exact packet flow will vary based on originating network, interface type, and timing within the transitional solution, GDIT's solution handles all scenarios with the proposed systems, with the eventual elimination of the transitional components when the full NG9-1-1 construct is enabled, including IP carrier trunks and the carrier-based Location Information Server (LIS). The planned NG9-1-1 data center routing is illustrated in Figure 30.

The Emergency Services Routing Proxy (ESRP) queries a location server leveraging the HTTP-Enabled Location Delivery (HELD) protocol and inserts location information into the SIP header (longitude/ latitude, civic address, or phase 1/2 cellular information). The location server in the transitional model as proposed by GDIT is the Location Database (LDB), constituted by both a private ALI/ANI and a private LIS. In the planned NG9-1-1 evolution, the LDB will be replaced by a carrier-deployed LIS. With insertion of location information, the ESRP will identify the PSAP routing based on the established Policy Routing Function (PRF). The Emergency Call Routing Function (ECRF) and the Location Validation Function (LVF) elements will then be queried to identify appropriate GIS mapping information using the LoST protocol, and insert a SIP URI in the packet header. Finally, the CPE will route to individual call takers and present the calling party information to the operator. For any location information that is presented by reference (mobile clients), the CPE will de-reference the location to a location value utilizing updated HELD queries to the LDB, ensuring that the call taker is presented with up-to-date mapping and location information.

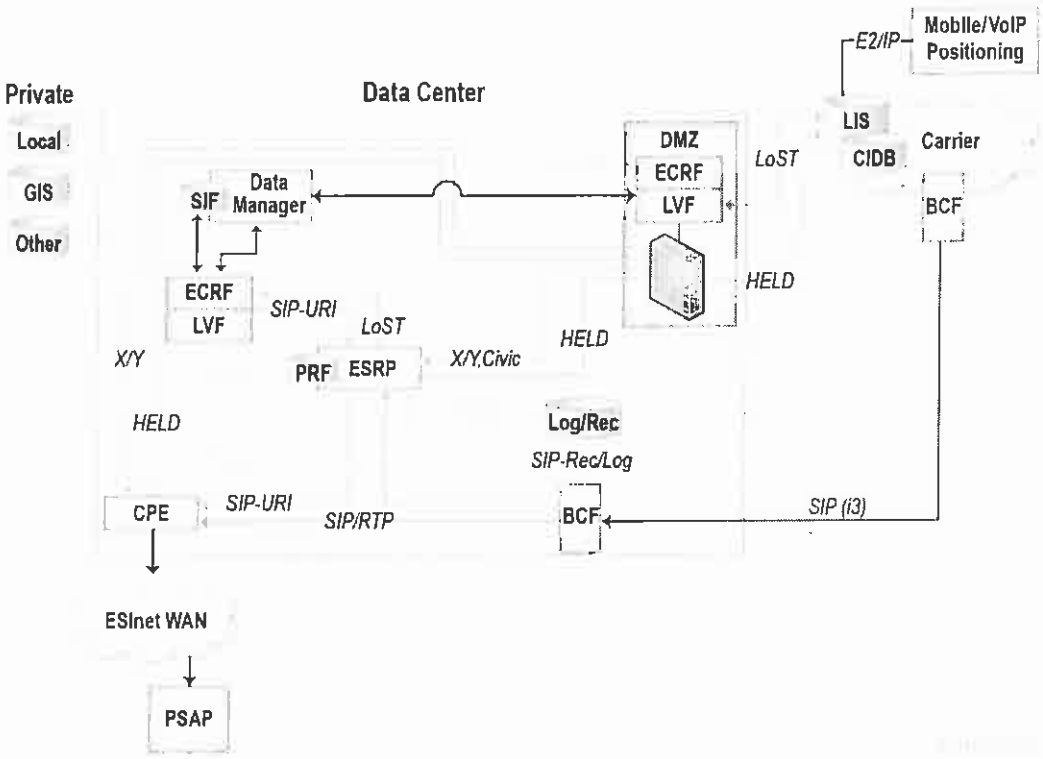


Figure 30. NG9-1-1 NENA End-State Architecture (Planned)

8.7.2. Connectivity

Call handling appliances within the PSAP will have the option of either displaying mapped ALI or connecting to an external GIS/mapping system within any PSAP.

Call handling appliances within the PSAP shall be able to connect to other public safety dispatch systems such as CAD and logging/recording systems.

The CallStation CPE will integrate with the DDTi mapping client to present real-time call specific mapping detail, including reference updates for mobile interactions on each call taker workstation. The DDTi mapping agent is integrated into the CallStation CPE to enable full coordination between the call taker position and the mapping interface. In this manner, single point-and-click of mapping entries are available, fully synchronized with the location database and the caller information. Detailed information on the DDTi mapping interface is provided in Section 8.7.23, Mapping.

In addition, the CPE solution includes a modular, templated, event-based system for outputting data to third-party systems, including centralized and local CAD. The data link layer of this interface may be either serial (i.e., RS-232) or Ethernet. GDIT's proposed solution includes a network addressable serial converter at each PSAP (as required) to provide serial CAD interface. The proposed CPE solution also supports a wide variety of Computer-Aided Dispatch (CAD) interfaces deployed in the field, including DSS recording solutions that are currently deployed. The number of CAD interfaces is expandable via IP to provide a near-limitless number of supported CAD outputs. GDIT's solution also includes an IP to serial adapter at each PSAP to perform network connectivity to legacy systems.

8.7.3. Customer Premises Equipment

The system shall have the ability to process the various payloads as may be presented by multimedia reporting party devices.

All descriptions of functionality shall be comprehensive enough to allow the State 911 Department to perform a detailed evaluation of system functionality, provide a clear and concise description of how the various functions operate from a call taker perspective, and be compliant with all applicable NENA standards for CPE. The CPE shall have a small form factor footprint to take up minimal space at the PSAP. The CPE shall have a minimum of a nineteen (19) inch screen. Bidders shall supply complete descriptions of CPE configurations as separate sections. Bidders shall describe whether the system utilizes open source or proprietary software/products and detail what, if any, are utilized. The response shall describe how product enhancement control is maintained independent of open source community advances. The response shall describe any risks associated with utilization of open source or proprietary software.

Bidders shall describe how they handle multiple payloads and how these payloads shall be presented to the call taker.

Bidders shall describe the system architecture with respect to the major components or modules, and describe how the system shall react to a failure of each major component or module. The response shall explain how the system meets the requirement to have no single points of failure.

The contractor shall employ security measures for the CPE, applications, and appliances at the PSAPs. These measures shall include physical safeguards, operating system hardening, hardware and software, information security best practices, stringent change management processes, security incident response, educational efforts and organizational policies.

GDIT is proposing the Emergency CallWorks (ECW) CallStation solution. The ECW solution includes i3 capabilities that provide voice and text capabilities today. The ECW CPE utilizes hosted architecture with call routing and services delivery occurring from the data center over the ESInet WAN, and received by the call taker workstation. The required workstation has low processing demand, allowing the use of a fully standard 32- or 64-bit Microsoft Windows-based PC. CallStation uses a standard Mozilla browser to provide all proposed multi-media payloads to call takers, and it does not require a client application. The DDTi mapping interface utilizes a thin client that fully integrates the CPE for ESRI-compliant mapping. DDTi mapping is defined in greater detail in Section 8.23, Compliance with Americans with Disabilities Act.

GDIT's proposed solution places Windows-based Dell Optiplex 3020 small form-factor workstations. This workstation is a longer life commercial level desktop providing an Intel 4th generation i5 quad core processor equipped with Window 8.1 operating system and 4Gb of RAM. This workstation will support all existing voice and text services, and all NENA-defined (current and expected future) documents, images, and video formats.

Each workstation will be equipped with:

- Dell 24-inch LCD monitors (qty. 2)
- Fentek Industries programmable keypad (KPP35U)
- Audio Interface Unit
- APC UPS
- APC Maintenance Bypass Panel (SBP1500RM)
- Soundbar (Dell AX510PA1)
- Cyberxlink 8-port Ethernet switch (2200-12651-025)
- Plantronics wireless headset (CS540-XD) (Optional)

Finally, each workstation and limited Secondary PSAP will be equipped with a Polycom SoundPoint 650 IP phone. These multi-line display phones will support all voice requirements, including both the NG9-1-1 voice and the administrative lines. The Polycom 650 is a commercial grade phone with the following features:

- Up to 6 lines
- 2 x Ethernet 10Base-T/100Base-TX Network Ports
- Quality of Service: IEEE 802.1p, IEEE 802.1Q (VLAN), Type of Service (ToS)
- Voice Codecs: G.711a, G.711u, G.722, G.729ab
- Monochrome 320 x 160 LCD display
- Dimensions (HxDxW): 5.9 in x 7.5 in x 10.4 in
- Built-in web server, on-hook dialing
- 4 programmable line buttons, 8 programmable buttons
- Call timer
- Call Services: Call Forwarding, Call Hold, Call Transfer, Call Waiting, Caller ID, Voice Mail
- Function Buttons: Headset button, Hold button, Menu navigation keys, Mute button, Redial button, Speakerphone button
- Hearing Aid compatible
- New message indicator
- Ringer control
- Digital duplex speakerphone
- Volume control
- Compliant Standards: AS/NZ 3548 Class B, CISPR 22 Class B, CSA 22.2 No. 950, EN 60950, EN55022 Class B, EN55024, FCC Part 15 B, ICES-003 Class B, UL 1950, VCCI Class B ITE

Representative workstation details are shown in Figure 31 and Figure 32.

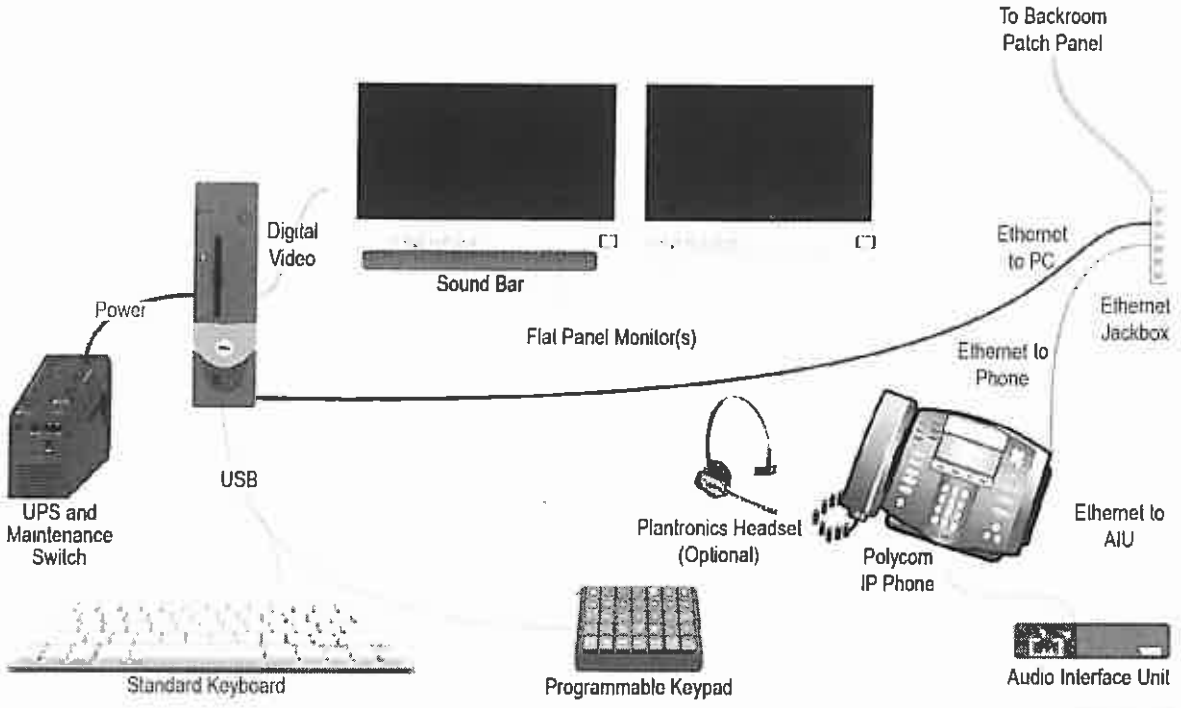


Figure 31. Call Taking Workstation Detail

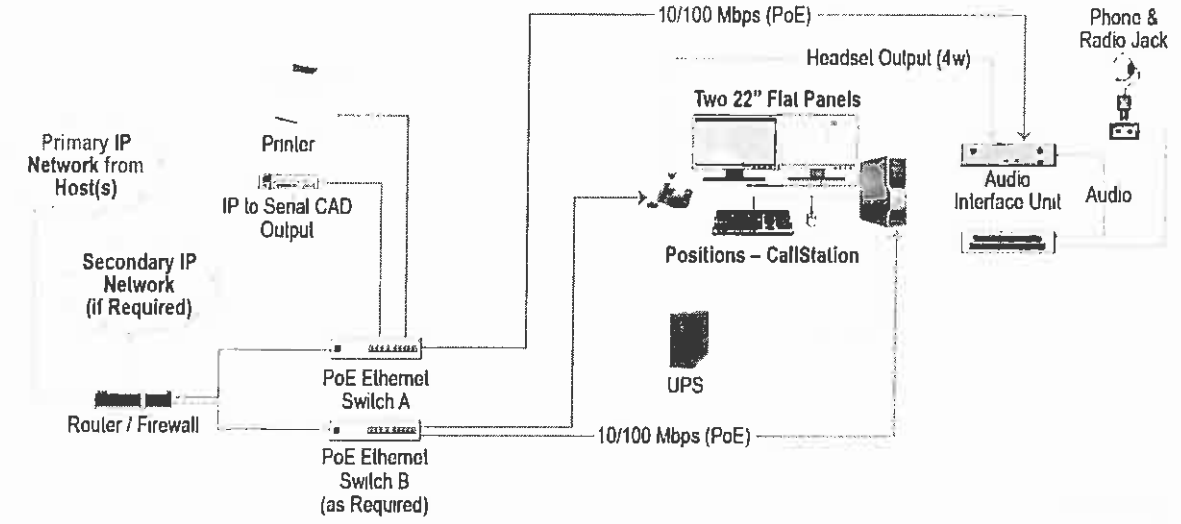


Figure 32. Typical PSAP Call Taking Workstation Networking

Workstation management is provided by integrating workstations with the AD environment for authentication and application of group policy. GDIT will collaborate with the Commonwealth IT/desktop organizations to develop and apply policies and practices consistent with Commonwealth's methodologies, as appropriate. Group policies will be managed centrally and focus on establishing restrictive privileged administrative access to system functions that pertain to security considerations, including call taker ability to add or modify software, system configurations, network connections, and other high-risk activities. Group Policy settings are

viewed by AD administrators using administrative template files (ADM or ADMX files) and the Group Policy Object Editor, or GPEdit (launched by running gpedit.msc). Using GPEdit, the administrator creates Group Policy Object (GPO) files. The GPOs are configured to apply (or not apply) to computers and users within the AD structure. There are a number of rules that GPOs must follow in order to function correctly.

Workstations will be provided with McAfee advanced endpoint protection that includes anti-virus and firewall. All updates will be managed through update services provided in the data center DMZ and applied through GPO rules.

GDIT has provided an alternate solution to placement of full desktop personal computers as call taker workstations by leveraging Virtual Desktop Interfaces (VDI). With VDI, all desktop applications and processing is placed centrally at the data centers, with intelligent thin or zero client terminals placed locally. In this client-server approach, all maintenance is moved to the data center, providing exceptional control for security. GDIT believes VDI best aligns with the Commonwealth's construct of centralization, commonality, security, and reduced operations and maintenance costs. GDIT has not chosen to propose VDI as our primary solution due to a level of uncertainty in the operational construct of the call takers.

The CallStation CPE proposed by GDIT is deployed in a hosted architecture, with all intelligent routing and services delivered from the data center. The CallStation platform leverages two levels of redundancy to ensure there is no single point of failure at either the systems level or the facility/network level. Within all/each data center, CallStation is deployed in a high-availability (HA) two-server cluster. Services to any PSAP are provided from the primary server, and failure of the active will be survived by the mate components without loss of any service capacity or capability. Each server cluster delivers 99.999% availability.

The second level of survivability provides a geo-diverse configuration across physically diverse data centers, each with a HA configuration in each data center. Where single and most multiple failures are survived within a cluster, catastrophic data center failure or network isolation will be survived through survivable-aware routing of traffic to the clusters at the alternate data center. Each data center configuration is sized to support approximately 120% of all traffic requirements, ensuring that each data center is capable of serving the complete needs of the Commonwealth. As long as one of the server locations is available and connected, workstations will function as expected.

All information needed by CallStation to properly support administrative actions and route traffic is managed across four databases within the clusters. Replication of this data within an HA cluster and across multiple data centers is performed autonomously by the service-aware clusters. Some of this replication is performed in real-time and some is performed in a periodic window, largely depending on the criticality of data needed to support data center survivability. GDIT includes in our proposal a 10 GB direct connection between the data centers that is the primary path for all database replication.

Payload Types

GDIT's proposed solution provides fully NENA-compliant NG9-1-1 support for the initial payloads, including voice, mapping, and texting (SMS/MMS) services. The CPE and all ESInet systems have been tested to also generically support most common documents, images, and

video formats without any significant change in system architecture, and most probably without any change other than software patches. NENA standards pertaining to protocols and methodologies for these payloads remain largely undefined, however, and work will need to be performed to integrate delivery of these payloads in a NENA-compliant manner within the ESInet. Specific to the CPE, CallStation utilizes a browser-based user interface, which will have little difficulty in supporting the delivery of any known payload types.

Open Source Software

Access to and control of all third-party software source code allows ECW to support the proposed solution on the timeline needed by the Commonwealth, not the timeline dictated by Avaya, Cassidian, Intrado, Dialogic, Microsoft, or any other third-party vendor. The proposed CPE solution product development is completely controlled and is completely free from third-party product end-of-life, road maps, and bug repair delays.

Because of the freedom and flexibility it offers, the proposed CPE solution utilizes open source extensively across the software stack. The internally developed Java Enterprise web application, which provides all 9-1-1 business logic that essentially acts as the ANI/ALI controller, is the only component which is not open source. All other software components of the system, from the operating system to the SIP stack, are derived from open source solutions.

The risks associated with utilization of open source software are comparable to and in most cases less than the risks associated with using closed source software. Several risks supposedly associated with the use of open source software are: security issues, patent issues, and maintenance issues. However, each of these purported issues is actually a strength.

Security vulnerabilities are more easily identified in open source software, which leads to quicker patch releases. The security record of widely deployed open source software versus closed source competitors speaks for itself. Patent liability and indemnification are problems for all software; Emergency CallWorks indemnifies the customer with regards to the entire solution. Software projects come and go, no different than commercial software vendors and products; however, open source provides ECW with the option to "self-maintain" third-party software in perpetuity.

- Major Open Source Components
- Spring Framework
- Apache Tomcat
- Hibernate
- MySQL
- Asterisk
- Oracle Java Runtime Environment (JRE)
- openSUSE Linux
  - Linux Kernel
  - GNU C Library
  - System V Init
  - Numerous OSS libraries

8.7.4. Applications and Appliances

It is not the intention of the State 911 Department to design or define the applications and appliances required by the system. However, bidders shall identify the applications and appliances included in the system, together with any virtualization technologies utilized.

GDIT's proposed solution leverages a mix of individual servers, blade servers, and virtualization to balance the needs of hardware reliability and architectural survivability with reduced space, power, and management. In all cases, GDIT has chosen to not virtualize those applications where increased risk of virtual machine failover could potentially reduce the availability or QoS that has been seen in some voice systems.

Table 6. Application Hosting

Application / Appliance	Virtualized	GDIT Team Partner
ESInet		
ESRP	Yes	Synergem
Legacy Gateway (LIF/ NIF)	Yes	Synergem
Legacy Gateway (PIF) digital	No	Aculab
Legacy Gateway (PIF) analog	No	AudioCodes
Border Control Function	No	Oracle
ECRF/LVF	Yes	DDTi
GIS Mapping	Yes	DDTi
Logging	No	DSS
CPE	No (Blade Servers)	ECW
Routing / Switching	No	Cisco
Firewalls	No	Cisco
Network and Security Management		
NTP	No	Spectracom
Domain Control	No	Microsoft
Authentication	Yes	Cisco, Microsoft
SIEM	No	AlienVault
Storage	No	EMC
VoIP QoS	No	Oracle
Network Monitor	Yes	SolarWinds
Element Management	Yes	Various
Imaging Server	Yes	Microsoft, EMC
Update Server	Yes	Various
Security Management	Yes	Cisco

8.7.4.1. Availability

The applications and appliances shall be housed in two (2) separate data centers within the Commonwealth, and possibly a third data center outside the Commonwealth. Each of the data centers shall have the capacity and operational readiness to support the entire system and load of the system shall one (1) or more of the data center(s) become inoperable.

The applications and appliances shall meet a 99.999% standard of availability in the system architectural design. Bidders shall describe how the system shall achieve this availability standard. Bidders shall include all required hardware, software, and services needed for a complete installation that can support the expected transaction volumes of call routing, location verification, and other functions and capabilities for a completely functional Next Generation 911 system and as defined within this RFR. The hardware, software, and databases upon which these applications and appliances will operate shall be capable of handling the anticipated transaction volumes with a one (1) second or less response time during peak operating hours.

GDIT's proposed solution places two geo-diverse data centers to host the ESInet applications and services and deliver all services to the remote call taker positions over the IP WAN network. The data center locations are specifically selected to provide:

- Extended geographical separation that minimizes the impact of regional disasters that could otherwise affect both locations
- Proximity to all major carrier interconnection points
- Proximity to Commonwealth-owned facilities
- Ability to support Tier 3 data center requirements
- Reduced transit and backhaul considerations for primary data center access to traffic

Each data center is configured initially to serve greater than 120% of the Commonwealth's identified service demands, and deployed in an HA configuration to ensure no single point of failure. Loss of any one system or service is survived by the mating HA component within the same data center. Should any single data center experience network isolation from the ESInet WAN or the carrier services, or experience a failure affecting multiple systems, the second data center – in part or by functional system – will serve to meet service demands. GDIT's proposed solution includes a dedicated, redundant 10G Layer 2 connection between all data centers (independent of the ESInet connections) that will support database and configuration synchronization and replication, and provide an alternate ESInet connectivity in the event of application, cluster, or data center failure or loss of data center connectivity to the ESInet.

GDIT is proposing the initial deployment of two data centers, and the optional deployment of a third data center, with each of the three locations capable of supporting the entire demands of the state, Where the ESInet and WAN routing of NG9-1-1 services fully supports the three data center configuration, the connectivity of inbound carrier traffic becomes a critical consideration, as discussed in Section 8.7.1, Routing Requests. The transitional environment exclusively affects the methods for connecting to the legacy carriers (TDM) and the means for gaining location information in cooperation with the carriers. However, the application environment has minimal differences from the NENA planned NG9-1-1 construct.

GDIT is proposing a multi-vendor, federated applications environment, where best-of-breed technology has been selected for each of the primary applications, including BCF, ESRP, ECRF/LVF, and CPE. The availability of each of these systems is assessed in both an inter-system HA and within architectural availability, leveraging redundant instances of the HA construct. The availability for each application component is described as follows:

- **Legacy Gateway (PIF)** – As discussed in Section 8.7.1 (Routing Requests), TDM traffic entering the ESInet (in the transitional environment) can be either analog CAMA, analog (robbed bit) T1, or SS7. CAMA circuits offer no failover protection and trunks would be duplicated and split over multiple physical gateways to protect against hardware failure. In this case, failure of a line card or circuit would be identified by the selective router and alternately routed over the second trunk. SS7 and T1 offer greater flexibility, where trunk groups are built over separate physical facilities. In this case, a given trunk is available on two separate devices, over two separate lines, and requires no rerouting by the originating

switch. With the duplication of all trunks and availability of all traffic at both data centers, all trunks will have at least four paths into the ESInet.

- **BCF** – The border controllers are deployed in an HA configuration with each data center, interfacing with either the PIF (gateway) or directly to the carrier via SIP. The Oracle BCF provides application layer service awareness using SIP options ping that identifies preferred routing both within a data center and across multiple data centers. Each interfacing device (PIF or carrier SBC) is configured to route to the preferred device and alternate devices at one or more data centers. In this manner, the four BCFs serve to provide HA across each device.

- **ESRP and Legacy Gateway (LIF/NIF)** – The Synergem ESRP is comprised of two individual HA cluster solutions. The first cluster leverages an HA web services pair in each data center, leveraging VRRP to dynamically route between the BCF and the web services servers. Failure of either BCF or web server will be protected. The second HA cluster supports both the LNG (LIF/NIF) and the ESRP, called the i3 Evolution servers. The i3 Evolution servers are independent instances that provide routing information, and any of the i3 instances can serve call routing purposes by placing the IP destination address in the web services server. Priority will be given to the i3 that are local to the web services servers. In this way, both data centers are running active-active for ESRP and LIF/NIF routing.

- **ECRF/LVF and LDB** – The DDTi ECRF/LVF and LDB are served from a three-server Windows data center edition cluster that virtualizes 17 machines over three physical servers. In this configuration, each virtual machine, utilizes server resources that are available, based on the health of the systems. Failure of any server will utilize spare capacity in the remaining server to deliver the required services. The cluster in each data center is deployed in a mated configuration, where all services can be delivered from either cluster, ensuring that the functions are HA within each data center and redundant across the two data centers. The only exception to this is that administrative services and LDB updates are delivered only from one cluster, and loss of this cluster would prevent database changes during a failure condition. All services, however, will function without impact to live service operation.

- **CPE** – As detailed in Section 8.7.3 (Customer Premises Equipment), the CallStation CPE leverages two levels of redundancy to ensure no single point of failure at either the systems level or the facility/network level. Within each data center, CallStation is deployed in an HA two-server cluster. Services to any PSAP are provided from the primary server, and failure of the active will be survived by the mate components without loss of any service capacity or capability. Each server cluster delivers 99.999% availability. Secondly, a mated pair of clustered servers is provided at the second data center, also in an HA configuration. Failure of the cluster in one data center, or isolation of the data center, is survived by the mated cluster in the second data center. While this failover does not preserve active call, new calls will be autonomously routed to the appropriate CPE cluster.

  It should be noted that GDIT has proposed an alternate solution intended for large PSAPs wishing to have a CPE cluster dedicated to their site placed locally. Should this alternative

be selected, the local CPE would route traffic across all call taker positions, and the mated cluster in the data center would provide redundancy.

- **WAN** – The ESInet WAN is comprised of two primary components: the 'core' transport network and the access loop (last mile) connection between each facility and the core network. GDIT has partnered with Windstream to provide comprehensive carrier services. The Windstream core network is a full MPLS mesh transport network, providing high-availability transport across private, leased, and multi-carrier facilities. Access loops utilize a mix of both Windstream and leased facilities, depending on availability of connections locally. Existing Local Exchange Carrier (LEC) T1 facilities are predominantly used on small to medium PSAPs as the least costly option for primary connections. Secondary connections (as required) will typically leverage alternate carriers, including the Commonwealth MBI network. Tertiary connections (as required) are typically designated satellite connections or as an alternate carrier wireline solution. All available connections between a site and the core network will be prioritized by GDIT's proposed edge devices based on achieving required performance and availability parameters, managed at the ESInet edge router.

GDIT's proposed solution includes a redundant 10G pipe between data centers that will serve as an alternate path for all system and applications, providing two critical functions:

- First, this connection serves to allow systems and services to synchronize between both data centers, including storage, databases, and routing tables such that all services can be supported from both data centers.
- Secondly, this connection provides network (WAN) alternate path survivability should primary ESInet WAN connections become isolated. In his case, applications delivered to PSAPs can be survived at the network layer, rather than initializing applications in the second data center.

GDIT's proposed solution is designed to be HA within each data center with the added reliability of architectural redundancy across multiple data centers. The following rationale highlights the primary considerations in the availability determination:

- **ESInet WAN Core** – The Windstream core network provides a full MPLS transport mesh with diverse routing across diverse facilities. Each data center (1 GB) connection will interconnect with a different edge router.
- **ESInet Access Loop Circuits** – Individual circuits are expected to provide 99.5% availability. Use of secondary circuits at a PSAP, including the use of diverse building entrance, diverse carriers, and non-collapsed facilities in the access loop or core increases the availability to 99.999%.
- **Data Centers** – All applications in the ESInet within each data center are provided in an high-availability configuration. GDIT's conservative assumption is that each individual server provides 99% availability, assuming a single power supply. Individual servers with dual power supplies provide increased availability, including the use of blade servers. The use of a two-server high-availability cluster (N+1) increases availability to 99.999%. The availability is enhanced by leveraging 'super clustering' (NxN) across multiple locations.

8.7.4.2. Application/Appliance Security and Authentication

All applications and appliances shall support the i3 security standards for authenticating users requesting services (call routing, payload delivery, etc.) from entities within and outside the ESInet. Bidders shall fully explain how authentication credentials shall be issued to entities that request services from the applications and appliances provided under this RFR and the methods employed to examine and authenticate a requester's credentials at the time that service requests are made. The contractor shall follow i3 standards for issuing credentials and authenticating user requests.

The contractor shall comply with NENA Security for Next Generation 911 Standards, including without limitation, NENA 75-001.

GDIT's Application/Appliance Security and Authentication solution will securely authenticate and verify users and devices into the MA NG9-1-1 system, supporting users, systems, services, and applications. Our commercial Certificate Authority (CA) will be integrated with the Microsoft Active Directory (AD) domain authentication platform that will contain Root CA services provided by VeriSign. This will facilitate secure encrypted access and validation of MA NG9-1-1 internal and external user authentication credentials. All MA NG9-1-1 system web application services that support Secure Sockets Layer (SSL) will utilize this authentication method where encryption, authentication, and signing functions are required. A Certificate Signing Request (CSR) will be generated on each of the MA NG9-1-1 application web servers, and submitted to VeriSign for SSL certificate provisioning. GDIT will work with all vendors to ensure that future enhancements to MA NG9-1-1 web-based applications and services are compatible with and support SSL encryption. Other applications, systems, and network-based resources that only support TACACS or LDAP authentication will leverage Microsoft AD authentication and Cisco TACACS authentication, allowing users to securely access these resources through the MA NG9-1-1 network, and then allowing subsequent administrative access to these resources.

GDIT's solution complies with NENA security standards as prescribed by the 75-001 guideline and with the i3 Security Standard for NG9-1-1. All network appliances will utilize a centralized TACACS authentication server to ensure all administration of network infrastructure components is performed by authorized personnel only. All network communications between geographically separated locations, such as PSAP and data centers, will be accomplished by leveraging encrypted Virtual Private Network (VPN) point-to-point tunnels, using Generic Routing Encapsulation (GRE) and Internet Protocol Security (IPsec).

8.7.5. Border Control Function

The system shall include a border control function that provides a secure entry into the ESInet for payloads presented to the network. The contractor shall provide redundant network appliances at each data center, including but not limited to, firewalls, routers, switches, and Ethernet cabling, as required, to ensure connectivity to the ESInet demarcation point, payload transmission upstream and downstream, and network security for each PSAP and for each of the data centers.

The BCF shall maintain functionality that identifies and authenticates payloads from approved service providers and prevents unauthorized access to the secure ESInet. Bidders shall describe in detail the system's BCF, including all devices required and any special issues of deployment that are anticipated. The BCFs shall be provisioned in a manner that assumes distributed denial of service and other attacks and has the ability to defend against such attacks while maintaining full call acceptance functions. The BCF shall be able to rate-limit traffic, both IP traffic and call (SIP) traffic across network-to-network boundary. Further, bidders shall include security parameters that extend through the ESInet to the point of demarcation within the PSAP. If the system is to be connected to the internet, bidders shall describe in detail the required bandwidth, number of recommended upstream internet

providers, and how these connections shall be protected against various attacks, including without limitation, distributed denial of service attacks.

As per NENA 08-003, the Border Control Function (BCF) is a Session Border Controller (SBC), which is an application-aware security device and voice firewall providing secure entry of IP traffic into the ESInet. The SBC components of BCF inspect, modify, and control SIP signaling and associated media where ESInet and agency networks interconnect and where ESInet connects with service provider networks. The Oracle (previously doing business as Acme Packet) Net-Net 3820 is the industry's leading SBC product family, which has been deployed globally for 12 years in mission-critical networks. GDIT has deployed numerous Net-Net 3820 SBCs at U.S. military and federal installations nationally and globally. The Oracle SBC mitigates security threats, resolves interoperability problems, and provides reliable SIP-based communications. The controller protects and controls real-time voice, data/text, and video NG9-1-1 sessions as they traverse IP networks between callers and PSAPs.

The BCF secures all voice traffic entering the ESInet. In most call flows, ingress traffic will enter the data center from the carriers, as either TDM or IP, and be routed to the BCF. In certain cases, emergency services traffic may enter the data centers through the Internet connections (including from the Mobile PSAP). Traffic that is destined for the ESInet that comes from the Internet will ingress the data centers through the DMZ to undergo appropriate inspection, and be routed to the BCF for entry to the ESInet with all other ingress traffic.

The proposed Oracle SBC is a purpose-built appliance that offers the following features:

- A one rack unit (1U) platform
- Redundant power supply and system architecture that leverages distributed multiprocessing with hardware-accelerated media functions.
- Network Equipment Building Systems (NEBS) compliant
- Supports up to 8,000 simultaneous sessions
- High Availability (HA) operation
- Hardware acceleration options for encryption, transcoding, and Quality of Service (QoS) measurement.

The 3820 as it relates to U.S. Department of Defense Security:

- Federal Information Processing Standards (FIPS) 140-2 compliant
- Defense Information Systems Agency (DISA) Unified Communications Requirements (UCR) compliant
- Listed: DISA Unified Capabilities Approved Product List (UCAPL)
- The Oracle SBC supports IPv6, IPv4, and IPv4-to-IPv6 SIP interworking.

The proposed SBC stops malicious Denial of Service (DoS) and DDoS attacks as well as controller overloads and other service impacting events while allowing valid traffic to pass through.

The Oracle SBC supports rate-limiting. The SBC component allows for aggregate bandwidth policies to be configured for each realm. A realm is a logical distinction that represents a route (or group of routes) reachable by the SBC. As the SBC processes call requests (to and from) a particular realm, the bandwidth consumed for the call is decremented from the bandwidth pool for that realm. Session capacity and rate limits are also configured for each destination. The SBC will deny any call request to a destination that has exceeded its configured policies for session capacity and session rate. The SBC may reject the call request back to the originator or reroute the call based upon configuration/policy. If multiple destinations are available, the SBC will check current capacity and rate for each destination and attempt to route the call only to destinations whose policy limits have not been reached.

Bandwidth requirements are driven by the amount of voice and video traffic. For example, a G711 call will consume about 100K of bandwidth, while video consumes much more.

The Oracle SBC supports many logical connections to service or Internet providers. Each service provider connection is represented by an IP address, or SIP trunk.

The product family is highly scalable and includes the industry's leading feature set, including:

- **Strong security** – Protects IP telephony and video sessions (prevention, detection, and reaction) and encrypts sessions to provide confidentiality. It stops malicious DoS/DDoS attacks as well as controller overloads and other service impacting events while allowing valid traffic to pass through.
- **Seamless interoperability** – Provides extensive signaling and media control features to overcome interoperability challenges that commonly occur when interconnecting third-party networks. It also performs interworking.
- **Assured reliability** – High availability and service quality features deliver reliable operations. They enforce QoS policies, balance loads across trunks, and reroute sessions around interface failures to optimize network performance, circumvent equipment and facility problems, and deliver service continuity.

The Oracle SBC hides both the network topology at both layer 3 (IP) and layer 5 (signaling). Topology hiding is mandatory to prevent the leakage of signaling and media topology to un-trusted network peers. Layer 3 topology hides via full source and destination Name Authority Pointer (NAPTR) of all session media. At layer 5, topology hides via an integrated SIP Back-to-Back User Agent (B2BUA). These functions ensure that the network signaling infrastructure is not compromised, which can lead to network piracy and/or DoS attacks against unprotected signaling elements.

The SBC protects privacy and confidentiality in several ways. The SBC enforces the privacy of user's identity through support of RFC3323 and RFC3325. We utilize encryption techniques such as TLS and IPsec to provide complete privacy of signaling information. Finally, the Net-Net protects service providers from leaking confidential signaling information, such as billing information, using programmable header stripping.

Net-SAFE functions/features:

- Topology hiding

- Network processor-based layer 1-4 hiding for signaling and media
  - Ethernet MAC + VLAN translation
  - L3 double-NAT translation
  - L4 double-NAT of TCP/UDP ports
  - Reset of TTL field, hiding the hop-count distance
  - Interception of ICMP ping/trace route
- Signaling processor-based layer 5-7 hiding
  - NAT for signaling messages and headers
  - Route stripping of VIA and RECORD ROUTE lists

- Privacy
  - Encryption – accelerator hardware module
    - TLS
      - Encryption – AES, 3DES, DES algorithms
      - Authentication – MD5 NULL, SHA NULL
      - Ciphers – TLS v1 ciphers
      - Range of key sizes
  - IPsec
  - Key exchange – IKE, manual
  - Protocols – ESP
  - Encryption – AES, 3DES, DES
  - Packet authentication – HMAC MD5, HMAC SHA-1
  - User identity and header privacy
    - SIP privacy (RFCs 3323 & 3325)
- Confidentiality: programmable removal and insertion of fields and headers

8.7.6. Emergency Call Routing Function

The system shall include an emergency call routing function that utilizes location information to route emergency calls to the appropriate PSAP. Bidders shall describe in detail the ECRF of the system and its relationship to other location-based call routing functions that may be offered by the bidder. Bidders shall detail the protocols used by the ECRF and shall cite the standards that the ECRF meets, along with the minimum requirement for GIS data.

GDIT is proposing DDTi's Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) solution. The ECRF/LVF will be used to provide location-based call routing utilizing the Location-to-Service Translation (LoST) protocol and provisioned GIS data provided by the Commonwealth. DDTi's combined ECRF/LVF is a single solution, scalable LoST server that adheres to Internet Engineering Task Force (IETF) and NENA standards. The ECRF/LVF is the location-based routing function in the proposed solution.

The LoST protocol is designed for servers to be organized in hierarchical trees, and for queries to automatically navigate the tree structure until the authoritative server for the queried location is reached. The ECRF/LVF fully implements these aspects of the LoST protocol and is interoperable in a tree structure with other authoritative LoST servers.

The tree structure of the LoST system allows GIS data to be maintained in any number of independent, authoritative datasets for different regions, each with its own logical ECRF/LVF

node. Because the Commonwealth already maintains GIS data as a single, authoritative dataset, GDIT proposes a single logical ECRF node provisioned with this dataset.

The proposed ECRF/LVF is hosted within Microsoft Internet Information Services (IIS), and connects to a Microsoft SQL server backend database. The solution leverages numerous Microsoft technologies to provide a highly available ECRF/LVF solution.

Error Handling

The ECRF makes every effort to answer queries with a useful response. If the queries contain a malformed request, an improper XML, an improper location, or do not follow the LoST protocol, or otherwise result in internal server errors or other anomalies, the server attempts to catch and categorize the error according to RFC 5222 section 13.1, and provides an appropriately constructed error response. Included in the message attribute of the response is the most precise description of the problem that could be determined. There are over 50 particular error conditions that are specifically checked when parsing requests alone.

Standards

The ECRF/LVF adheres to the following standards:

- IETF RFC 5222, and RFC 4848 compliant for LoST server implementation and discovery
- Supports service names identified in IETF RFC 5031
- Supports IETF RFC 5491 and RFC 5139 as they pertain to location profiles used in LoST
- NENA 08-003 version 1 compliant for both ECRF and LVF
- Supports data loads from the NENA GIS database schema for NG9-1-1 and other GIS data formats
- Supports NENA 08-003 v2 (draft) logging interface for all requests and responses
- Database uses Open Geospatial Consortium SQL standard (Microsoft SQL Server 2008 Spatial)

The ECRF has been tested for interoperability at several NENA Industry Collaboration Events (ICE), including ICE 3, ICE 4, ICE 5, and ICE 8.

GIS Dataset Requirements

Road Centerlines Layer

Road centerlines are required for use in the ECRF/LVF and are essential for the PSAP map display. The road centerlines layer must include the following minimum attributes:

- An integer unique ID
- Name fields, including prefix, name, type, and suffix
- Political division fields, including state, county (or equivalent), and incorporated municipality (if applicable), for both left and right sides of the road

The following attributes are strongly recommended for the road centerlines layer:

- Address range to/from values for both left and right sides of the road, oriented according to the direction of the road geometry

Address Site/Structure Layer

Address site/structure points are strongly recommended for use in the ECRF / LVF and PSAP map display, and must include the following minimum attributes:

- An integer unique ID
- An integer house number
- One of the following:
  - Name and political division fields, including street prefix, name, type, and suffix, state, county (or equivalent), and incorporated municipality (if applicable), OR
  - A reference unique ID field, indicating a road centerline from which to inherit the name and political division fields

Service Boundary Layers

A service boundary layer (polygons) is required for each service (RFC 5031) that is to be implemented. At a minimum, this must include the top-level service, urn:service:sos. Additional layers for sub-services (e.g., urn:service:sos.police, urn:service:sos.fire) are only required if calls are to be routed separately for those particular sub-services. GDIT and DDTi acknowledge and affirm compliance with the requirement in this section for full support of these sub-services.

Each service boundary layer must include the following minimum attributes:

- An integer unique ID
- Display name
- Service number
- SIP URI

Coverage Regions

In order for LoST servers to interoperate in a tree structure, as described above, each authoritative server must be provisioned with its coverage regions and the coverage regions of any immediate child nodes. For this reason, a geodetic coverage region layer is required. This layer must include:

- One or more polygons representing the Commonwealth's border, including any off-shore areas for which the Commonwealth is responsible

Civic coverage regions are maintained as tabular data. These coverage regions may be described in terms of political (country, A1, A2, A3, A4, A5) or postal (county, A1, PC, PCN) Presence Information Data Format Location Object (PIDF-LO) elements. Coverage regions can also be used to provide granular control over default routing responses from the ECRF/LVF. DDTi will work with the Commonwealth to develop appropriate civic coverage region data.

Additional NENA Data

The NENA NG9-1-1 data model is expected to list a number of additional attributes in the above layers as mandatory. While these attributes are not strictly necessary in order for our ECRF/LVF

to operate, it is strongly recommended that these fields be populated in accordance with the NG9-1-1 data model.

GDIT will assess the structure of the existing GIS data and provide instruction to the Commonwealth for any attributes which must be added or modified in accordance with the requirements above.

Bidders shall describe in detail the methodology that will be employed by the system's ECRF to process location information to determine the appropriate PSAP. The methodology description shall specifically address the GIS datasets that will be provided by the Commonwealth. Bidders shall detail how the ECRF shall utilize the mix of point and street centerline information that will be provided to the ECRF.

Locations in NG9-1-1 can be in the "civic" or the "geodetic-2d" profile. For geodetic locations, query processing is straightforward: the location is compared directly against the service boundary polygons for the requested service and suitable substitute services. If there is a single intersecting polygon, the server returns a mapping for that polygon. If there are multiple intersecting polygons, the server can be configured to return multiple mappings or a single mapping based on criteria such as the greatest area of intersection.

The ECRF/LVF features the ability to provision temporary "override" polygons to facilitate dynamic call rerouting for special events, large-scale emergencies, or other occasions. These polygons overlay those provisioned via normal service boundary layers, rather than modify them, so that temporary changes are isolated and easily reverted. When one or more temporary override polygons are encountered during ECRF/LVF query processing, the server will return the override polygon of greatest priority.

For civic locations, query processing first attempts to match the location to a known GIS feature, or set of features, and then compares the geometric representation of those features with the service polygons in a similar fashion to the geodetic query processing described above.

The civic location-matching algorithm uses a "best available information" approach to identify civic locations in LoST queries. This approach first attempts to make the most complete match possible to the location in the query, but falls back to less-specific data if a suitable match cannot be made. Specifically, the server first attempts to match the location to features in the address site/structure layer. If a match cannot me made, the ECRF/LVF will attempt to match the address to an appropriate range in the road centerlines layer, and then consider all segments, matching solely by name if necessary. If that fails, the ECRF/LVF will check municipal boundaries, if provisioned.

As a last resort, the ECRF/LVF can be configured to return a default route based upon tabular coverage regions. These coverage regions are based on political elements such as state, county (or equivalent), or municipality. Coverage regions and default routes can also be defined using postal elements, such as postal community name and zip code.

The ECRF/LVF has a modular design so that the precise location query logic can be fully customized if desired. Such customization is not expected to be necessary and is not included as part of this proposal, but is supported by the ECRF/LVF design to ensure maximum flexibility and adaptability to future needs.

The system shall include the following optional ECRF function: in addition to the service type "sos", the ECRF shall fully support a LoST that finds service messages for fire, police, and emergency medical services service types.

and shall support additional find service types (e.g., poison control, etc.) depending on the service area boundaries provided to the ECRF.

The ECRF/LVF fully supports the service naming conventions defined in RFC 5031, including the top-level services and sub-services defined therein. This proposal includes configuration of map layers for all of the services explicitly defined in RFC 5031, which include sub-services for fire, police, ambulance, and poison.

Service substitutions are also supported, and may be configured to return a mapping for an alternate service if the desired service is not available for the queried location. For example, if the ECRF/LVF receives a query for urn:service.sos.physician, but no physician service is defined for that location, the ECRF can be configured to respond with a mapping for another service, such as urn:service.sos.

The DDTi ECRF/LVF also supports the use of a single, configurable service name for querying additional data associated with a location. The service name given for this purpose in NENA 08-003 is urn:nena:service:AdditionalLocationData. To support this functionality, an address site/structure layer must be present in the GIS data, and must include an attribute containing the additional data URI for each address.

8.7.7. Emergency Services Routing Proxy

The system shall utilize an emergency service routing proxy for call delivery to the appropriate PSAP based upon location and routing rules. Bidders shall describe the system's use of the LoST protocol and how it interacts with the overall operation of the ESRP. Bidders shall describe in detail the system's process for the functions related to the ESRP and shall indicate any outstanding issues that the system may have with this process (as it is specified in the standards referenced in this document).

The Emergency Service Routing Proxy (ESRP) is the call processing and initial routing service in the i3 architecture. GDIT proposes the Synergem EvolutionNET ESRP to be deployed in a high-availability solution at each of the data centers.

The Synergem EvolutionNET ESRP is the call processing service in the i3 architecture. The ESRP is a SIP routing proxy that conforms to NENA's i3 specifications for the routing of 9-1-1 emergency calls in a "privately managed" NG9-1-1 IP/MPLS network. The EvolutionNET ESRP implements a Policy Routing Function (PRF) that evaluates the Policy Routing Rules (PRRs) to determine the appropriate "call treatment" as referenced in i3 standard and RFC 3265, which describes the SIP-based notification mechanism to obtain the value of the variables (LoSTServiceURN Condition). All SIP-based emergency calls pass location information either by value (PIDF-LO) or by reference (Location URI) plus a 'Service URN' to an ESRP to support routing of emergency calls. The ESRP passes the Service URN and location information via the LoST interface to an Emergency Call Routing Function (ECRF), which determines the next hop in routing a call to the requested service. The ECRF performs the mapping of the call's location information and requested Service URN to, for example, a 'PSAP URI' by querying its data and then returning the URI provided. Using the returned URI and other information (time-of-day, PSAP state, etc.), the ESRP then applies policy from a Policy-based Routing Function (PRF) to determine the appropriate routing URI. The general functions of an ESRP are described in NENA 08-002, Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3), with a more robust description provided in Section 5.2 of 08-003. In its present form, 08-003 version 2 adds text governing the disposition of calls forwarded by a PSAP to a responder in Section 5.2.1.1, which provides an overview to the functional description of the ESRP, and

deletes text in Section 5.2.1.5 (Policy Routing Function) describing the rule variables that may be used by the ESRP.

Fundamental routing capabilities of the EvolutionNET ESRP include:

- Accepts emergency calls from an upstream routing proxy, such as a carrier resident ESRP, LNG, or a BCF on the edge of an ESInet.
- Supports processing of emergency calls where the location information is specified in a civic or geodetic format. Using a provisioned ECRF, it determines the destination address (URI) to which the emergency call is to be routed.
- Supports processing of emergency calls where the location information is specified using a "Location by Reference" format. Using a provisioned LIS, it will obtain the de-referenced location. It will then use the de-referenced location information in a query/response interaction with the provisioned ECRF, incorporating the PRF and responding with a destination address.
- Supports a PRF to determine potential emergency call routes. A query/response interaction with a provisioned ECRF is a minimal action resulting from a rule governing the call origin. Other rules the PRF can apply govern call termination and can include a route decision based on knowledge that a particular downstream ESRP is busy (call queue full) or that a particular PSAP is offline.

The EvolutionNET supports (at minimum) the following interfaces for upstream/downstream communication:

- SIP call interface over UDP, TCP, or TCP/TLS.
- Location to Service Translation (LoST) interface for a provisioned ECRF. It maintains a persistent TCP/TLS connection with the ECRF and is provisioned with the credentials for the ECRF.
- HELD de-reference interface for a provisioned LIS. It maintains a persistent TCP/TLS connection with the LIS and is provisioned with the credentials for the LIS.
- HTTPS clients for the "AdditionalCallData" services. These services may be invoked when the ESRP receives a call with a "CallInfo" header with a "purpose" of "emergencyCallData," "emergencyCallerData," or "emergencyPSAPdata." The resulting data structure is an input to the PRF.
- Supports both the server and client side of the "ElementState" event notification packages. The ESRP maintains "Subscriptions" for this package on upstream or downstream elements it serves. These "State" interfaces supply inputs to the PRF.
- Logging interface for every transaction and message received and sent on its call interfaces, every query to the ECRF and LIS and every state change it receives or sends. For each call it will log the route decision and rules applied to determine the route.

As described in NENA 08-002, the EvolutionNET can be deployed as a primary, intermediate, or terminating ESRP, and it can serve as a primary interface to originating networks to route emergency calls to the next hop, such as an intermediate ESRP. As an intermediate ESRP, it will accept emergency calls from a primary ESRP and route them to another intermediate ESRP, terminating ESRP, or PSAP. Deployed as a terminating ESRP in larger PSAPs or PSAP cluster environments, the Synergem EvolutionNET ESRP serves as an outgoing call proxy for calls originating from within the supported PSAP(s). If the call is destined for another PSAP or agency, standards-based SIP call routing methods are used.

The proposed ESRP supports a PRF to determine potential emergency call routes. A query/response interaction with a provisioned ECRF is a minimal action resulting from a rule governing the call origin. Other rules the PRF can apply govern call termination and can include a route decision based on knowledge that a particular downstream ESRP is busy (call queue full) or that a particular PSAP is offline.

8.7.8. Location Validation Function

The system shall include a location validation function that shall be available to validate location information in order to ensure proper routing to the appropriate PSAP in at least the following instances:

GDIT's proposal includes the deployment of the DDTi Location Validation Function (LVF) as an essential part of the NG9-1-1 architecture. The primary purpose of the LVF is to validate call locations prior to an emergency call being routed by the ESInet. In a purely transitional legacy environment, validation will occur between the internal LVF to the internal location database LDB. This validation will include validation of Service Order Input (SOI) changes made between the service provider and the internal LDB. In the final Next Generation construct, an external LVF will validate call locations with the service provider LIS or other i3 agents. GDIT's proposed solution includes both an internal and an external LVF to support the extended migration from a purely legacy and purely i3 end-state environment, which could take many years.

The LVF is built on the same core and fully supports the same standards as the ECRF. Currently, the LoST protocol does not provide a means to separate LVF queries from ECRF queries. The queries are absolutely identical except that an LVF will always have the optional "validateLocation" flag set to true, where an ECRF query may set this flag to either true or false. There is no mechanism to conclusively identify the intent of the LoST query (ECRF or LVF).

Additionally, all LoST queries must be answered with a mapping from the authoritative server for a given location. In order for this to happen, LoST servers work together in a hierarchical "tree" and redirect to or recursively query other LoST servers based on coverage regions. Coverage regions designate authoritative server names based on service and location, and do not further differentiate based upon query intent.

Finally, in order for a LoST client (or server acting recursively) to actually make a query to any server in the LoST hierarchy, that client must start with the server's application unique string (name) and use U-NAPTR to resolve the URI of the target LoST server. U-NAPTR resolution using the registered (RFC 5222) application service and protocol tags for LoST also does not provide a method to resolve LoST servers separately based on query intent.

For those reasons, the ECRF and LVF implementations are not separable, even though they are commonly considered to be different functions. As a consequence, all ECRF and LVF servers must perform a dual role as both an ECRF and LVF, and deployment plans must size ECRF and LVF servers to handle the combined load within the desired performance parameters.

One ECRF/LVF server cluster will be deployed and be designated to handle traffic originating external to the ESInet. This server cluster is provisioned for use by service providers and user agents that are external to the ESInet.

An additional ECRF/LVF server cluster will be deployed at each data center and be designated to handle traffic originating internal to the ESInet. This will ensure that in the event that the publically accessible ECRF/LVF servers are overloaded or disabled, call routing functionality within the ESInet will be preserved. The internal servers will be used by the Location Database (LDB) in order to validate location and to ensure proper routing during a 9-1-1 call.

Figure 33 depicts the ECRF/LVF cluster within the DMZ, as well as a cluster within the ESInet. This diagram only shows one data center, but the architecture is duplicated within both data centers.

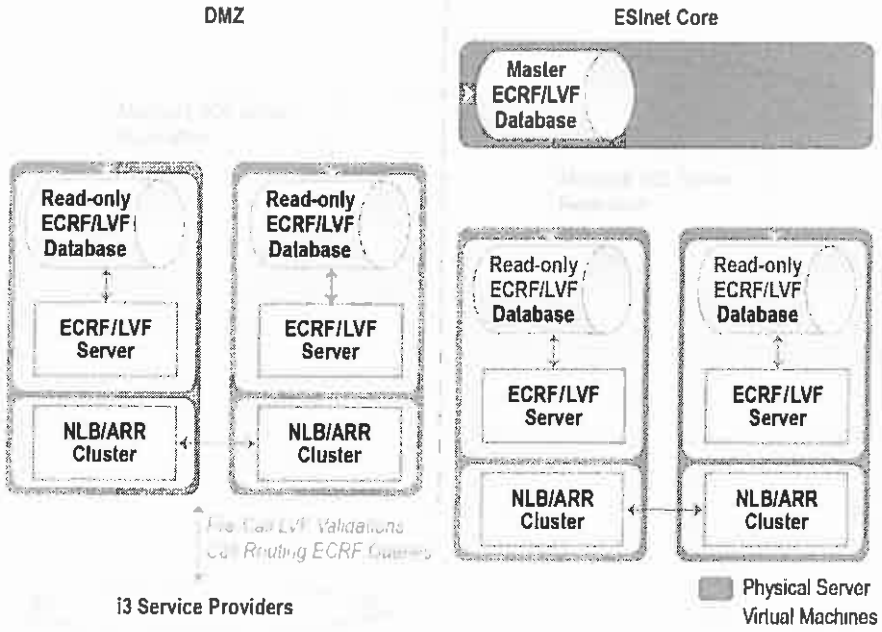


Figure 33. ECRF/LVF Cluster

At the time that service is ordered for a fixed location device (e.g., land line phone). The system shall extend an i3 standard interface using the LoST protocol to service providers that enter new customers into their databases such as an i3 compliant Location Information Server (LIS). Bidders shall explain how the system shall support this interface to their proposed LVF.

A public-facing ECRF/LVF server group will exist at each data center that is designated for handling queries that originate outside of the ESInet. These servers will be part of the same SQL Server replication tree as the internal ECRF/LVF servers and, therefore, will contain identical data. The border control function (BCF) will allow externally originating LoST queries from any

source *unless* the BCF deems that traffic to be malicious in nature. The authoritative coverage regions of the ECRF/LVF will be exported to a higher level ECRF/LVF node or Forest Guide.

Service providers will initiate a LoST query for all new locations, and queries for locations that fall within the area for which the Commonwealth is authoritative will resolve to and be answered by the public-facing Commonwealth ECRF/LVF server. It is expected that service providers will revalidate their entire location database at periodic intervals and the resulting revalidation queries will be handled in the same manner.

At the time that a nomadic device (e.g., VoIP phone) is connected to the network. The system shall extend an i3 standard interface using the LoST protocol to service providers that provide nomadic device services. Bidders shall explain how the system shall provide a real time interface to their proposed LVF that can be used to validate a nomadic device's location at the time that service becomes initially available to nomadic devices and subsequently any time the location of the nomadic device changes.

Service providers supporting nomadic devices will interact with the same public facing ECRF/LVF as service providers offering fixed devices, described above. Service providers will initiate a LoST query for all new and changed locations for nomadic devices, and the ECRF/LVF will respond in real-time.

Whenever a reporting party describes an emergency event's location that is not at the location of the device used to report the event (e.g., a structure fire across the street, a traffic accident previously passed on a roadway, etc.). Bidders shall describe how the system shall provide a real time interface to the PSAPs that can be used to validate location information entered by PSAP personnel.

The internally accessible ECRF/LVF server group will handle queries from PSAP call taker software. For locations that fall within the area for which the Commonwealth is authoritative, the server will provide a response including location validation. For locations that fall outside of this area, the server will perform redirection or recursion according to the LoST protocol in order to find an answer from an external authoritative server. The entire process of resolving an external authoritative server and completing the LoST query is expected to occur in real-time.

The LVF shall be provisioned with the same geographic datasets as the proposed ECRF. Bidders shall specify the relationship between the LVF and the ECRF and identify any unique GIS data requirements.

Both ECRF and LVF are provided using a combined implementation, and any ECRF/LVF node must be capable of providing the full call routing and location validation responses for its authoritative region. Multiple replicas will be used to support the reliability and availability requirements defined elsewhere, and all replicas representing a given authoritative region will use identical GIS data.

8.7.9. Rules-Based Routing Proxy

The system shall have a rules-based routing proxy functionality. Bidders shall describe how the system's rules-based routing interfaces to the other components making up the i3 architecture. Bidders shall specifically identify the interface used by the PSAP to establish these rules and any conditions that may exist limiting its function.

The Emergency Service Routing Proxy (ESRP) is the call processing service in the i3 architecture. The GDIT team will provide a high-availability ESRP solution as one of the functional elements of the ESInet within each data center, which will also support the multimedia call-answering solution provided in this proposal.

The ESRP uses the Policy Routing Function (PRF) to determine the next hop in routing a call. The PRF makes this determination by accessing the Policy Routing Rules (PRR) which are

designated by the PSAP/9-1-1 governing authority. Two documents should be referenced when developing Policy Routing Rules: NENA 71-502-v1, Overview of Policy Routing Rules, and NENA-STA-003, NENA Standard for NG9-1-1 Policy Routing Rules. The latter document describes the minimum set of rules necessary for development of a new NG9-1-1 system. The GDIT team actively participates on NENA's Policy Routing Rules (PRR) Working Group, which developed these documents, and wishes to make the Commonwealth aware that work has begun on the development of an additional document governing the operational aspects of designing Policy Routing Rules. This document will also be considered when developing Policy Routing Rules.

When the actual rules are developed during the course of implementation, the GDIT team will work with the designated 9-1-1 authority to incorporate the defined rules into the Policy Store that is accessed by the PRF. The user interface for the ESRP and PRF is presently provided in a tabular format. This interface is planned for update to provide a web/HTML interface for a future release. GDIT will work with the Commonwealth to customize the look and function of this interface to support user needs.

Additional detail on routing is provided in Section 8.7.1, Routing Requests.

8.7.10. Call Distribution

The system shall be equipped with a call control management module that provides Automatic Call Distribution (ACD-like) functions. The system shall be equipped with an IP-enabled call distribution function. The system shall provide the following minimum functions, and any additional call functions shall be identified by the bidder:

Call Transfer that shall include payload transfer

Consultation Hold

Minimum of Three Party Conference

System-wide and Local Instrument Speed Dial

Station-to-station Intercom

Supervisor Barge-In

Caller ID for equipped administrative lines

Direct-Outward Dialing

Toll Restriction, by area code, by station line

Support 4-Wire administrative Tie Lines

Support 2-Wire Ring Down Circuits

Caller ID to Telephone Sets

Abandoned Call Back

PSAP to PSAP intercom functions

Silent Call Procedure

TDD/TT/TTY call processing

The Emergency CallWorks CPE solution was designed and built from the ground up as a 9-1-1 call handling system. The solution includes NENA i3 call handling capability in the current version, and the system is designed to be software based, network-centric, and next generation ready from the very beginning. The solution includes all necessary equipment, software, and capability to take 9-1-1 calls directly from the Local Exchange Carrier (LEC), collect location information related to the call, present the call for answer at the PSAP, and provide all call

control capability. The system is fully integrated and includes advanced call control and Automatic Call Distribution (ACD) functionality necessary for handling 9-1-1 calls, including:

- **Automatic Call Distribution**. The ECW system includes ACD, including queue statistics reporting as an integral part of the solution at no additional cost. Emergency CallWorks has built a modular ACD system with pluggable support for various queue disciplines; thereby additional custom disciplines may be added by ECW at any time. The system supports advanced features such as Forced Answer, Zip Tones, automatic Wrap-Up time, and multiple Not Ready states.

- **IP Enabled**. The ECW CallStation solution was developed from the ground up to take advantage of the proposed NG9-1-1 infrastructure. ECW designed its solution on VoIP switch technology and then added the ability to interface to legacy telephony 9-1-1 delivery as opposed to adding digital technology on top of legacy systems. Our ability to comply with i3 is inherent in our system design. In addition, our solution has been designed to notify users and display Next Generation messaging (i.e., text, e-mail, video) as these standards are further defined and deployed.

- **Transfer with Payload**. The ECW system supports 'on-network' IP transfers which are orders of magnitude faster than traditional transfer methods and transfer all call data instantly with the call. On-net transfers provide the receiving PSAP all call history including the original ring-start time, all call events (e.g., Hold, Mute, Conference, etc.), as well as any notes from earlier call takers.

- **Hold**. All calls can be placed on Hold with a single action. In certain cases, calls can be placed on automatic hold to facilitate answering of a subsequent call. An unlimited number of calls may be placed on hold. If configured, ALI rebids will continue being updated while the call is on hold. When any call is retrieved from hold, the most recent ALI information is automatically presented to the user.

- **Conference**. CallStation supports several modes of conference creation including standard Conference and Conference-Transfer, Silent Monitoring, and Barge-In. The system may be configured to automatically Mute transmit to the last original 9-1-1 caller at the time a third party is conferenced; this feature allows for a private consultative transfer. Consultative conferences allow two local parties to speak without being heard by the 9-1-1 caller. Up to 120 conferences and up to 12-party conferences are supported on each CallStation cluster.

- **Speed-Dial**. An unlimited number of speed-dial entries can be associated with customer-defined categories. These entries can be configured to reach various destinations using different call paths depending upon the call type (9-1-1, Admin, IP, etc.). The system can also support Selective Transfer tandem codes. The speed-dial directory includes configurable hot buttons and real-time full-text search.

- **Barge-In**. The CallStation provides Barge-In functionality as part of robust call conferencing capabilities included with the solution. Call takers are able to "barge" into an existing call through a simple right-click menu option. As with all conferencing features of the system, there is no degradation in audio quality (regardless of the number of

participants), and all advanced features such as Telecommunications Device for the Deaf (TDD), Dual-Tone Multi-Frequency Signaling (DTMF) transmission, etc. continue to work the same as a simple two-party call. All information about the call including ANI, ALI, and event logs are displayed to the barging user immediately upon connection to the call. Every user who participates in the call in any way will see the caller's ALI information on the GUI and on the IP telephone.

- **Station-to-Station Intercom**. An unlimited number of speed-dial entries can be associated with customer-defined categories. These entries can be configured to reach various destinations using different call paths depending upon the call type (9-1-1 callback, Admin, PSAP on-way, etc.). The system can also support Selective Transfer tandem codes.

- **Caller ID**. CallStation fully supports Bell 202 type (U.S. standard) Caller ID including both Caller ID Number and Name. This data is made available throughout the system including on the PC display as well as on the backup phone display. Similarly, the Cisco CallManager, providing inbound/outbound will deliver inbound Caller ID, with the option of enabling or blocking outbound Caller ID. The Polycom phone display with present all call ID information on the LCD screen.

- **Direct Outward Dialing**. Direct Outward Dialing is provided for administrative calling both from the CallStation CPE and through Cisco CallManager located at each data center. Administrative calling (inbound and outbound) will be integrated into the call taker position, allowing click-to-dial (callbacks, station-to-station, conferencing, etc.) and providing full logging and recording, with integrated reporting on call statistics. Cisco CallManager provides both inbound and outbound administrative calling using both or either the local carrier trunks and the data center trunks. CallManager provides survivable local gateway capabilities on each PSAP ESInet edge router to ensure availability of administrative calling through local trunks even if the ESInet connection is lost.

- **Toll Restriction**. Outbound calling from any NG9-1-1 workstation will be routed by the CPE to utilize the administrative PBX and outbound trunks, leveraging integration with the Cisco CallManager Express (CME) placed at each data center. The CME supports a variety of toll restriction capabilities, including Class of Restriction (COR), restrict call attempts based on the incoming and outgoing criteria to block calls (for example, calls to 900 numbers), and allowing different restrictions to call attempts from different originators. For SIP phones, multiple COR lists can be applied under the voice register pool.

- **Tie Lines**. CallStation integrates with third-party administrative PBXs using a variety of interface types including Analog Telephone Adapters (ATAs), T1-PRI, and Session Initiation Protocol (SIP). Four-wire Ear and Mouth (E&M) tie-lines are not supported natively, and they require the use of an external gateway. The use of SIP trunking is strongly recommended for the best integration.

- **Ring Down Lines**. CallStation supports a wide variety of types of analog and digital line interfaces by utilizing COTS gateways. The system provides support for both wet and dry ringdown lines for varying purposes such as remote extensions and door phones. As with

other line types, the system can support a practically unlimited number of ringdown circuits.

- **Abandoned Call Back**. Calls which disconnect before answered (Abandoned Calls) are tagged with an "Abandoned" status, appear blue and are sorted to the top of the list of calls available for answer. If Mapping is used, the ANI with an icon will also appear on the map until cleared or recalled. Recalling (callback) is accomplished via a simple click on the call list or map icon. If the call is from an uninitialized cell phone that does not provide a valid callback number, the abandoned call will automatically be cleared from the abandoned call queue. The system is also able to automatically determine if the call should be dialed back as a local or long distance call; this is especially important with 80+% of all call being wireless. ALI lookup is processed as a part of the callback.

- **Silent Calls**. CallStation includes a single button for initiating a TDD Challenge. The standard challenge message is customer configurable, allowing the call taker to comply with a Silent Call SOP with a single button click. Full time DTMF detection, logging, and display are also provided. All DTMF tones sent or received are time and user stamped and logged to the Call Detail. These logs are displayed in real-time in the Call Activity window and may be retrieved indefinitely as part of the Call Detail Report.

- **TDD/TTY**. The ECW system manages Telecommunications Device for the Deaf (TDD) detection and processing as an integrated software function from within the VoIP (data center) engine, eliminating the need for specific TDD hardware or software at the call taker position. the call taker can communicate with TDD and Text Telephone (TTY) devices directly from their workstation keyboard and the CallStation softphone application. TDD calls do not have any feature limitations or restrictions compared to regular voice calls. TDD calls may be placed on hold, transferred, and conferenced including the ability for multiple call takers to participate in the TDD session. CallStation provides both Hearing Carry Over (HCO) and Voice Carry Over (VCO) for all TDD calls. HCO and VCO are included at all times throughout the call and the call taker is not required to configure any settings for such.

8.7.11. Legacy Gateways

The State 911 Department expects that legacy gateways (both PSAP and network) will exist outside of an ESInet, and the State 911 Department envisions a period of time that legacy gateway services may be required by the State 911 Department. Bidders shall provide an effective and efficient solution to the provisioning of legacy gateway services.

Legacy gateways are critical components of the transitional NG9-1-1 environment, allowing connectivity between carriers using TDM (legacy) interfaces. The core of all legacy gateways includes the software-based Location Interface Function and Network Interface Function (LIF/NIF) routing interface and a hardware-based TDM-to-IP conversion gateway (PIF). As articulated in Section 8.7.1 (Routing Requests) and illustrated in Figure 34, the type and quantity of PIF interfaces is highly dependent on each carrier's ability and agreement for terminating with the Commonwealth. GDIT's proposed solution includes all three gateway functions and the ability to contract or expand quantities as greater definition from the carrier terminations becomes apparent. However, we have made assumptions on the quantities that are based on the GDIT team's experience and awareness of carrier intensions. Based on these assumptions, GDIT's proposed solution includes:

- Equipped capacity at each data center to support 25% of all egress carrier traffic as analog CAMA (MF), with placement of the PIF at each data center or at locations that optimize carrier interconnection and transport.
- Equipped capacity at each data center to support 75% of all egress carrier traffic as digital T1 or SS7, with placement of the PIF at each data center or at locations that optimize carrier interconnection and transport.
- Equipped capacity at each data center to support greater than 200% of all egress carrier traffic as IP/SIP, with placement of the terminating BCF at each data center.

8.7.11.1. Legacy Network Gateway

The LNG shall provide connection to the legacy system components utilizing pieces of the legacy system infrastructure, including the existing ALI data management system and the two (2) in-state redundant selective routers.

The LNG shall attach sufficient information to the call, such as location and callback number, for handling within the ESInet.

Bidders shall describe the LNG within the ESInet environment and its approach to sizing this component.

When TDM trunks are provided from a carrier to deliver 9-1-1 traffic to the ESInet, IP gateways – termed Proxy Interface Function (PIF) – serve to terminate the trunks, convert the traffic to NENA-compliant IP, and allow the traffic to enter the ESInet. The PIF is one of the three functional components of each legacy gateway, including the Legacy Network Gateway (LNG), Legacy Selective Router Gateway (LSRG), and Legacy PSAP Gateway (LPG). The two additional components of the Legacy Gateways are the Location Interface Function (LIF) and Network Interfaces Functions (NIF). The LIF and NIF are software functions necessary to support a transitional environment where location information in not provided by the carriers (through the LIS) and, therefore, requires a transitional construct for accessing and inserting location information (termed PIDF-LO). GDIT's proposed solution utilizes a Location Database (LDB) to serve as both ALI and LIS in the transitional environment.

As fully described in Section 8.7.1 (Routing Requests), GDIT must pursue interconnect agreements with carriers to identify the connectivity methods for incoming traffic to both (and possible third) data centers. Figure 34 reflects the three primary interconnect methodologies. Legacy connections supported by re-pointing existing CAMA from individual PSAPs to terminating at the data centers is expensive for both carriers and the Commonwealth. Due to timing, potential regulatory concerns, or technology limitations, however, CAMA does represent the least complex solution in terms of coordination with the carriers. In this case, GDIT proposed solution provides PIF capacity to terminate approximately 350 CAMA trunks at each data center initially, or 25% of all identified traffic demands.

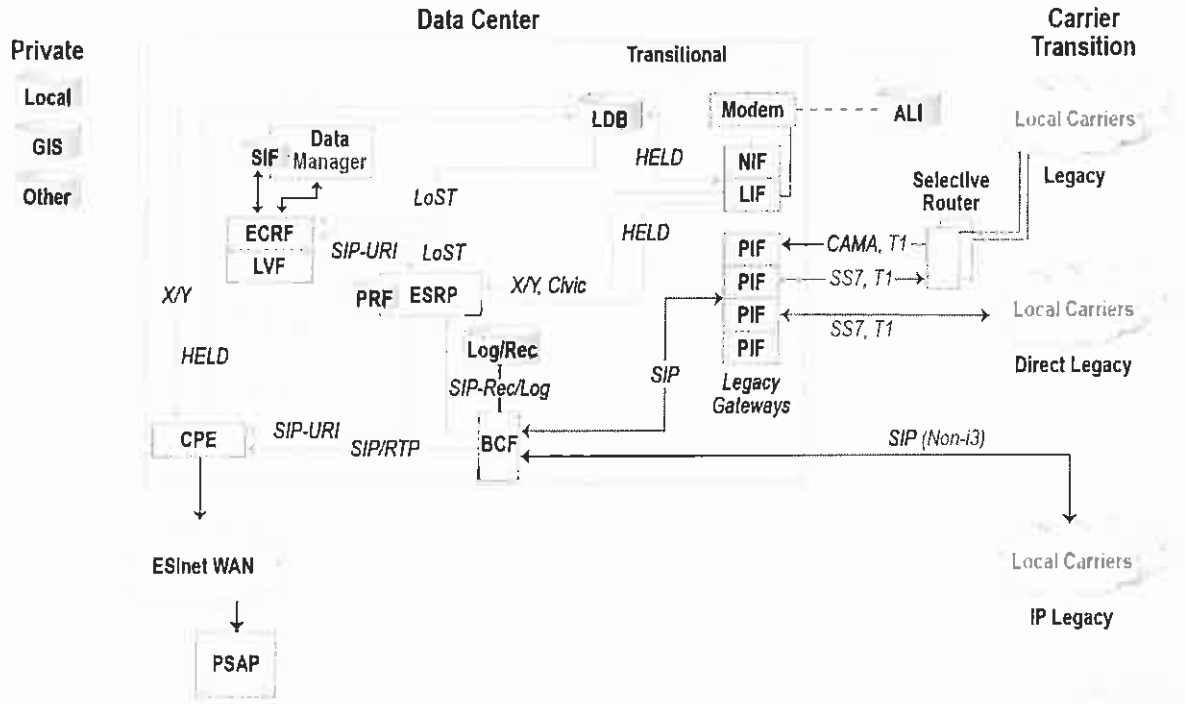


Figure 34. Connectivity Methods for Incoming Traffic to Data Centers

Direct legacy transition methodology provides direct connectivity with carriers (bypassing the selective routers), leveraging higher density interfaces, including T1 and SS7. SS7 offers significant advantages of defining trunk groups across multiple PIFs, allowing for full protection in the event of a hardware failure and across data centers. Transport of T1 and SS7 is certainly more efficient than CAMA, although more expensive and complex than IP to duplicate and transport. GDIT's proposed solution has equipped each data center to terminate 75% of all traffic demands using T1 or SS7.

The IP legacy transition provides direct connectivity with each carrier using SIP and eliminating the need for the PIF. In this methodology, the BCF terminates the SIP trunks. GDIT believes most carriers will support and enable IP legacy connectivity initially as a cost reduction to both their own network and to the Commonwealth. As each carrier agrees to connect using IP, the number of PIF interfaces is reduced. The BCF is equipped and capable of supporting up to 8,000 simultaneous sessions.

The LIF and NIF functions of the LNG are provided to support 1,000 simultaneous trunks at each data center. These licenses are independent of the type of interface provided by the carrier (via PIF).

The LNGs will be designed as high-availability pairs in each data center with terminations from each SR pairing to each data center to ensure the overall architecture meets the availability requirements of the Commonwealth.

The LNG provides connection to the legacy system components by utilizing pieces of the legacy system infrastructure and replacing the existing ALI data management system with the proposed Location Information Function (LIF) and Location Database (LDB).

The end-state NENA i3 architecture anticipates that all IP-based calls entering the ESInet will already have location, either by value or by reference, attached to them. It is also expected that service providers will allow the functional elements within the ESInet to query the service provider's Location Information Server (LIS) to dereference location when it has been provided by reference.

Service providers, when implementing a LIS, must provide NENA i3-compliant reference mechanisms, and ultimately provide location in the form of a PIDF-LO.

During the transition to full NENA i3, however, location must be supported for legacy wireline, wireless, and VoIP calls. Currently the ALI database is used in E9-1-1 networks to provide this data. Using the ALI database in an i3 environment presents numerous challenges. Of particular note are the quality of the data and the response times of ALI queries. To properly steer a 9-1-1 call in i3, it is essential that location data be pre-validated using the Location Validation Function (LVF). At present, most ALI databases are not well synchronized with the GIS data, and ALI database providers have no mechanisms or processes in place to perform LVF validation or to fix the errors. It is also critical to note that location must be available early on in the call flow (unlike E9-1-1, where the ALI database is not queried for location until the call is already at the PSAP). The call cannot be properly steered through the i3 functional elements until location is available. This makes it critical that at least coarse location information is available in milliseconds, not the 2-5 seconds it can take to query a typical hosted ALI database.

To overcome the problems highlighted above, and following NENA recommendations, GDIT's proposal includes the LIF within the LNG in conjunction with the LDB to serve as both a private ALI and offer the supplemental information included in the LIS. The advantages of using the LDB are that all location records must pass LVF validation, and the LNG can receive location data in just milliseconds, so routing of the call will not be delayed.

8.7.11.2. Legacy PSAP Gateway

The system shall provide connection to the legacy system during the transition to the Next Generation 911 system, and for some private safety departments and secondary PSAPs through a legacy PSAP gateway, or LPG. The LPG shall support an IP interface towards the ESInet on one side, and a traditional multi-frequency (MF) or enhanced MF interface (comparable to the interface between a traditional selective router and a legacy PSAP) on the other. The LPG shall include an ALI interface (as defined in NENA 04-001 or NENA 04-005) that can accept an ALI query from the legacy PSAP, and respond with location information that is formatted according to the ALI interface supported by the PSAP. If an emergency call routed via the ESInet contains a location reference, the LPG shall support a de-referencing interface to a LIS or LNG or ingress LSRG to obtain the location information that will be returned to the legacy PSAP in the ALI response, if required. To populate non-location information in the ALI response, the LPG may need to support an interface to a call information database. The LPG may also support an interface to an ECRF which it can use to determine the transfer-to party under certain selective transfer scenarios.

The LPG shall provide special processing of the information received in incoming call setup signaling to facilitate call delivery to the legacy PSAP, to assist legacy PSAPs in obtaining callback and location information, and to support feature functionality that is currently available to legacy PSAPs, such as call transfer and requests for alternate routing.

Bidders shall describe in detail its solution for the LPG within the PSAP environment. The contractor shall provide a migration plan for phasing out the LPG as PSAPs are converted to the Next Generation 911 system.

The legacy PSAP gateway is a NENA-defined component that allows legacy (E9-1-1) call taker positions to be served within the ESInet construct. In this approach, any legacy PSAP that is connected to the ESInet will not need to upgrade E9-1-1 call taker workstations during the

transition phase to receive caller information, and it also allows full E9-1-1 operational control, including managed transfer to both NG9-1-1 and E9-1-1 PSAPs.

GDIT is proposing a migration approach that deploys the 'common' ESInet infrastructure, including data centers, ESInet routing with transitional components, core ESInet WAN, and network and security operations. Individual PSAPs, based on a coordinated schedule, will be integrated into the new common infrastructure through last mile connectivity and the addition of new (PSAP-specific) call taker infrastructure. During this parallel period, full performance testing can be performed and local operational staff can train and improve familiarity without disruption to live operations or systems. The actual migration only occurs when egress 9-1-1 traffic is rolled from terminating at the PSAP to terminating at the data centers. The use of parallel systems also provides a mechanism for rollback should the PSAP experience any problems, until the legacy systems are decommissioned.

Because the network is not undergoing a systemic 'flash cut', but rather being rolled out on an individual PSAP basis, those sites that remain served by the selective router will continue to receive and process traffic without any change in existing systems or operations. Call transfer from an ESInet (NG9-1-1) PSAP to a non-ESInet (legacy E9-1-1) PSAP will occur through the Legacy Selective Router Gateway (LSRG), with referring traffic appended with the appropriate ALI/ANI formulation through the PIF interfaces within the data centers. An LPG is only required at an individual PSAP in cases where local selective router trunks must be moved and/or disabled locally (with corresponding traffic sent to the data centers) before the local legacy call taker (E9-1-1) consoles are upgraded to NG9-1-1 workstations.

GDIT's migration strategy intends to upgrade PSAPs to new NG9-1-1 systems and ESInet connections prior to removing the local selective router trunks, thereby making an LPG unnecessary. GDIT understands that (at least) the Commonwealth Safety Departments will fall outside of the NG9-1-1 modernization initiative, and we have provided the LPG systems as optional hardware components of our solution These optional components will share the use of the LIF/NIF software licenses that are included within our LNG solution, licensed to support 1,000 simultaneous calls at each data center. Again, this would only be required in cases where egress 9-1-1 circuits have been moved before the legacy E9-1-1 consoles have been upgraded. GDIT notes that, with ESInet connectivity provided, the cost of upgrading four (4) E9-1-1 positions to NG9-1-1 workstations is roughly equivalent to the cost of implementing an LPG at that PSAP.

8.7.12. Location Information Service Interface

The system shall have a LIS interface.

Bidders shall describe in detail the LIS function. NENA i3 Standards specify that the LIS is not resident inside the ESInet and is the responsibility of the originating service provider. However, the location information server function may not immediately be available from the communications service provider. In the interim, the contractor shall provide a similar product or service in order to begin the location validation process before the delivery of a call. This location information may be presented as either actual location or location reference of any and all endpoint devices. Bidders shall detail their solution for this functionality, including where the LIS service sits in relation to the ESInet and all necessary security mechanisms, detail the interactions between the LIS and ECRF, and clearly define the roles and responsibilities of the contractor and the State 911 Department and/or Commonwealth in the maintenance and administration of the LIS. Bidders shall also describe the transition steps to transition carrier data into the LIS. The LIS function shall have an automated reporting mechanism to escalate any discrepancies or fallout between the LIS and ECRF. Any deviation from the LIS as defined herein should be noted

and the proposed functional element fully explained. The contractor shall take all action necessary to transition to the LIS, including without limitation, working cooperatively with the enhanced 911 service provider, communication service providers, and carriers to accept data, and contracting with the incumbent local exchange carrier for ALI database services as may be necessary.

The Location Information Server (LIS), as defined in NENA 08-033 v1 and v2 (draft) is outside of the ESInet and the PSAP and is the responsibility of the service providers. It is defined that, in the final NENA-compliant NG9-1-1 construct, all IP-based calls entering the ESInet will have location, either by value or by reference included. It is also defined that service providers will allow the functional elements within the ESInet to query the service provider's LIS to dereference location when it has been provided by reference (e.g., mobile clients). Service providers, when implementing a LIS, must provide NENA i3-compliant dereference mechanisms, and ultimately provide location in the form of a PIDF-LO.

During the transition to full NENA i3 construct, location must be supported for legacy wireline, wireless, and VoIP calls. Currently the ALI database is used in E9-1-1 networks to provide this data. Using the ALI database in an i3 environment presents numerous challenges. Of particular note are the quality of the data and the response times of ALI queries. To properly steer a 9-1-1 call in i3, it is essential that location data is pre-validated against the LVF. Most ALI databases at present are not well synchronized with the GIS data, and ALI database providers have no mechanisms or processes in place to perform LVF validation and to fix the errors. It is also critical to note that location must be available early on in the call flow (unlike E9-1-1, where the ALI database is not queried for location until the call is already at the PSAP). The call cannot be properly steered through the i3 functional elements until location is available. This makes it critical that at least coarse location information is available in milliseconds, not the 2–5 seconds it can take to query a typical hosted ALI database.

To overcome the problems, NENA recommends the use of the LIF within the LNG utilizing an internal location database with data steering data. This private database is often referred to as an LDB, or Location Database (NENA 77-501 and NENA-INF-008.1). The LIF is a logical component of the LNG, although it can be physically separated. It is expected that this function will reside in the same location as the LNG, on the border of the ESInet. In this proposal the LDB will fully replace the existing ALI database and include a supplemental information available from support datasets to provide LIS-like services. The advantages of using the LDB are that all location records must pass LVF validation (discrepancy workflow is described in more detail in Section 8.7.13, ALI Database Services), and the LNG can receive location data in just milliseconds, so no holding up of the call is needed. In essence, the LDB function takes the role of both traditional ALI and a next generation LIS. As the LDB function defined here takes both the role of the LIS and ALI database management system, some of this text may be duplicated in the response to Section 8.7.13.

Why an LDB and not a LIS:

- While the LDB and LIS are very similar, an LDB supports legacy service providers in an i3-compliant manner. A LIS is designed for pure i3 location delivery. As an example, the LDB is required to support SOI processing, while a LIS is not. This means legacy providers can continue "business as normal," without having to change their existing processes.

- NENA recommends the use of an LDB and not a LIS within the transitional environment for legacy providers.

The LDB location data is maintained via the continued use of Service Order Input (SOI) processing. The LDB SOI processing supports both NENA 2.1 and NENA 4.0 formats, as well as custom service provider specific formats. When used in conjunction with the Location Validation Function (LVF), the LDB validates all records in a SOI file before committing the changes to the database. In the event of validation failure, a SOI error record is created and returned to the service provider, as well as the agency responsible for the maintenance of the GIS data used in the LVF. In this regard, the LVF replaces the function of the MSAG used in legacy E9-1-1 systems.

During the transition period, service providers do not have to change the way they operate with regard to populating a location database. Prior to transition, they would submit SOI files to the ALI database provider. During transition, they will continue to provide the same SOI files, only now the data will be loaded into the LDB. The LDB is expected to be more strict in terms of the quality of the data – due to the LVF validation checks – so initially service providers may see more SOI failures than they are accustomed to.

Call Flow When Using an LDB

It is important to understand call flow and how the LDB fits in when processing legacy 9-1-1 calls. The following sections describes the role of the LDB for both wireline and wireless 9-1-1 calls.

Legacy Wireline Call

When a person dials 9-1-1 from a wireline device, the call will be delivered to the 9-1-1 network LNG or converted to SIP by the service provider and delivered over IP. In either case, location information for the wireline call will need to be determined. If the service provider chooses to deliver the call over SIP, it is their responsibility to provide a LVF valid location with the call.

During the transition period to NG9-1-1, the LDB will be hosted and supported by the 9-1-1 authority, much like traditional ALI systems are today. The LDB will provide near identical functionality to traditional ALI systems. It is expected that the service provider delivering the wireline 9-1-1 call will provision the LDB, using the SOI interface, with the phone number (TN) and civic address of the wireline subscriber. Alternatively, providers can manually edit their own records using the LDB web interface. The LDB web interface provides secure access to the LDB database for service providers to access their own records. Provisioning of the LDB is described in more detail in Section 8.7.13.

When the wireline 9-1-1 call reaches the LNG, it will contain the wireline subscriber's telephone number, or ANI. The LNG or other device requiring location will then query its provisioned LDB server via the LIF, using the HELD protocol, for the civic address of caller. The returned civic address will be subsequently used in the call flow to query the ECRF in order to route the call to the appropriate PSAP.

Legacy Wireless Call

When a person dials 9-1-1 from a wireless device, such as a mobile phone, it will be delivered to the 9-1-1 network LNG or converted to SIP delivered over IP. In either case, location

information for the wireless call will need to be determined. If the service provider chooses to deliver the call over SIP, it is their responsibility to provide a LVF valid location with the call.

It is expected that the LDB will be configured with one or more connections to the appropriate Mobile Positioning Centers (MPCs) in order to obtain a refined location (equivalent of wireless phase II location data). When the wireless 9-1-1 call reaches the LNG, it will contain a unique identifier (based on the originating cell tower and sector) in the form of either an Emergency Service Routing Key (ESRK) or a combination of an Emergency Service Routing Digits and Callback Number. The LNG or other i3 component that may need location information (for example, the CPE may query the LDB directly for location rebid information), constructs a HELD query and sends this to the LDB. Based on the information in the HELD query, the LDB constructs an E2 query to request location information from the MPC. It is likely, based on current technology, that the E2 query will be slow. In that case, the LDB will send the LNG the location of the cell tower as an initial response. Once a response is received from the MPC, the LDB will provide the "phase II" location data for any subsequent location requests or location dereference requests. However, the LNG will use the initial returned location to query the Emergency Call Routing Function (ECRF) in order to route the call to the appropriate PSAP in a timely manner.

The LDB must be properly provisioned with steering data. This steering data includes Pseudo Automatic Number Identification (pANI) information, and details the MPC connection that is responsible for handling this pANI. This steering data is configured using the LDB web interface.

Error Handling

The LDB makes every effort to answer queries with a useful response. If a query contains a malformed request or an improper XML does not follow the HELD protocol, or otherwise results in an internal server error or other anomalies, the server attempts to catch the error and provides an appropriately constructed error response as defined by the HELD protocol. Included in the message attribute of the response is the most precise description of the problem that could be determined.

Logging

The LDB logs all queries and responses. Reports may be generated from these logs and provided to system administrators at regular intervals. All location information errors will be made available to the Commonwealth and any authorized providers in an agreed upon format.

8.7.13. ALI Database Services

The contractor shall provide ALI database and related services to include, but not be limited to, establishing, housing, installing, activating, operating, and maintaining an ALI database system for the duration of the contract and any renewals thereof; providing access for input, removal and/or update of records by carriers; updating of selective router databases; interface with and steering of ALI requests to external database systems; acceptance of inquiries from PSAPs; providing reports as prescribed and detailed by the State 911 Department; and coordinating efforts with EOPSS/OTIS and/or with carriers to assist with network and interoperability issues should they arise. The contractor shall provide file extracts (daily, weekly, or full file) to the State 911 Department upon request of the State 911 Department at no additional charge to the State 911 Department.

The contractor shall make available, through a subscription-based service, subscriber list information data to eligible entities that are providers of emergency services and providers of emergency support services for the

purposes of delivering or assisting in the delivery of emergency services. The form of the proposed agreement with eligible entities shall be approved by the State 911 Department. All requests for this subscription-based service shall be approved by the State 911 Department. Subscription service shall allow for automatic downloading, via electronic means, of subscriber list information records by geographic region with a frequency of daily or weekly updates. Subscriber list information and data shall be used solely for public safety purposes.

As described in Section 8.7.12 (Location Information Service Interface), the LDB will provide both ALI and LIS location services within the transitional environment. The LDB location data is maintained via the continued use of Service Order Input (SOI) processing. The LDB SOI processing supports both NENA 2.1 and NENA 4.0 formats, as well as custom service provider specific formats. When used in conjunction with the Location Validation Function (LVF), the LDB validates all records in a SOI file before committing the changes to the database. In the event of validation failure, a SOI error record is created and returned to the service provider, as well as the agency responsible for the maintenance of the GIS data used in the LVF. In this regard, the LVF replaces the function of the MSAG used in legacy E9-1-1 systems.

For legacy wireless devices, the LDB supports location determination over the E2 protocol to a MPC. It is important to note that a call will not be held up while the LDB queries the MPC, as the typical MPC response time would produce an unacceptable delay. Detailed location information will be requested from the MPC in the background (i.e., phase II location), but the call will continue to flow into the ESInet using coarse location data provided from the LDB based on pANI shell records (i.e., cell tower location). The LDB will be provisioned with the appropriate steering data so it can make the correct decision on which MPC to query based on the pANI.

For both legacy wireline and wireless, the LDB can provide location information to authenticated clients, such as LNGs and LPGs, using the HELD protocol. The LDB will not directly provide updates to the Selective Router (SR). In cases where the SR remains in the call path for an updated PSAP, GDIT will work with the SR owners to perform the necessary update of circuits, as part of the PSAP migration process. Where direct connections from carriers are provided, eliminating the SR from the call path, GDIT will work with the SR owners to eliminate all translation information from the routing database.

The LDB supports the following standards:

- NENA 08-003 version 1 compliant
- IETF RFC 6155 compliant
- IETF RFC 5985 compliant
- Supports the use of IETF RFC 3966 tel URIs representing global (E.164) numbers for device identification. IETF RFC 5222 compliant for LVF validation
- Full logging of all transactions
- NENA E2 protocol support for wireless device location determination

Figure 35 shows a simplified system architecture, where the LIF/LDB is queried by an LNG.

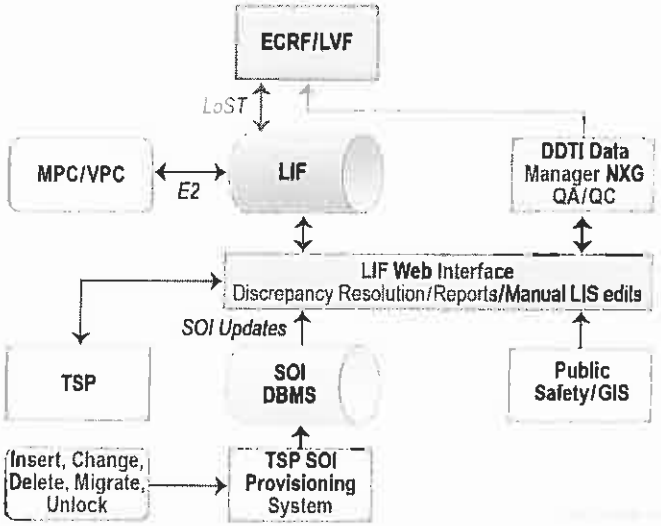


Figure 35. Transitional Location Flow for Legacy Network Gateway

The LDB will be deployed in geographically diverse high availability configurations using the same technique as the ECRF/LVF. The primary data center location will be responsible for the processing of SOI records. Replicated copies of the database at both data centers will be used for answering HELD queries. Each data center will also support the E2 connections to the MPCs. At least two LIF/LDB servers will be deployed at each data center in a virtualized environment. Each LDB server has its own Microsoft SQL Server database backend and runs completely isolated from other LDB server databases (there is no interdependency to ensure maximum uptime).

Service Order Input Processing

In order to successfully replace a legacy ALI system with a LDB, a mechanism must be provided to the service providers to update the location information in the LDB. During the transition to i3, and to aid 9-1-1 authorities gaining cooperation from the service providers, the LDB system includes a Service Order Input (SOI) processing function that is similar to existing SOI processing. This means that the service providers do not have to change current processes in order to support the i3 system.

Service providers can submit their SOI files for processing via some agreed upon, secure method. Asynchronous back end server processes run to process the SOI files. Multiple SOI processing agents can be configured on a single database, allowing multiple SOI files to be processed at the same time.

Unlike SOI processing for E9-1-1 ALI databases, each SOI record must be validated against the GIS, by way of an LVF, prior to the record being committed to the database and being made available for HELD queries. This ensures the civic address location provided by the service provider can be mapped, and thus routed and plotted. If a record fails validation, the service provider is notified (various notification mechanisms exist, including an error report). The group responsible for the GIS map data can also be notified, so the map data can be checked for accuracy.

Scheduled, periodic revalidation of existing LDB records will also be performed by the system. This process checks all LDB records that have previously been flagged as LVF valid, and submits a new LVF query to verify each record is still valid. Records that fail validation will be flagged in the LDB as invalid, but will still be returned in HELD queries for a configurable period of time (by default, this is 30 days), allowing the service provider or GIS department time to investigate and resolve the issue. The screenshot below shows the report for the revalidation.

Web Interface

The LDB utilizes a web-based interface that allows authorized personnel access to the backend location database. From this web interface, users with the appropriate permissions can schedule reports and data extracts to be run.

Key functionality of the web interface

- Role-based security, restricting what users can do and what data they can see. For example, a service provider will only be allowed to view their location records and job reports from SOI jobs they have submitted.
- Ability to query data by telephone number and address.
- Ability to modify location records and validate the changes against the LVF in real-time.
- View reports.
- Workflow for resolving data discrepancies for records that have failed LVF validation (for example, if, after review, the service provider has determined that the location data is correct, the discrepancy can be routed to MassGIS for resolution).

The Commonwealth will have the ability to define users via the LDB web interface. Users will have permission-based access to their subscriber data and be able to schedule daily data extracts. There are no additional charges or subscriptions required for this functionality while the LDB is supported under maintenance.

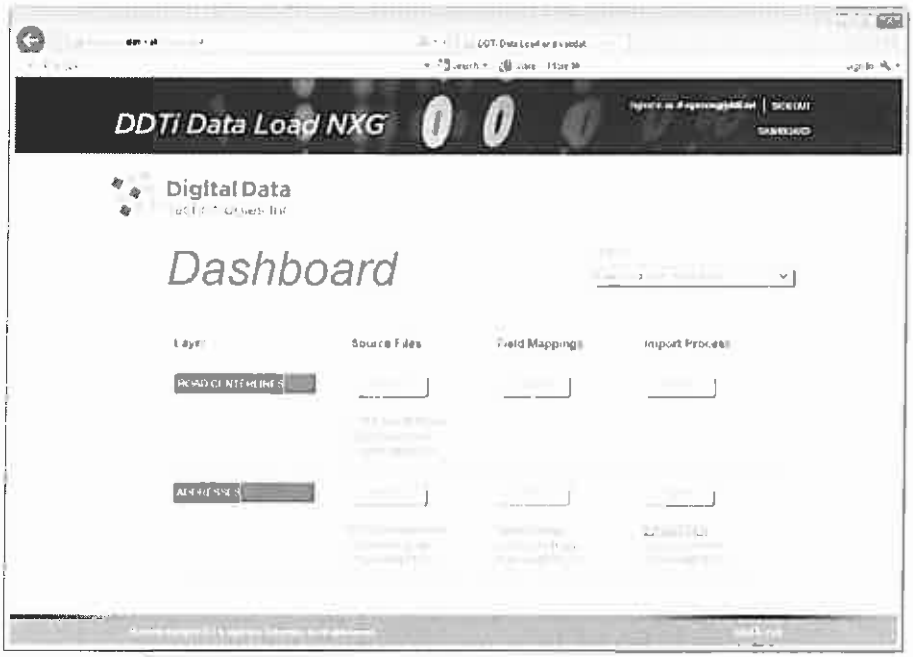
8.7.14. Spatial Information Function

The contractor shall provision and populate the SIF with the geospatial data provided by MassGIS and periodically as required to keep the data current. The SIF will then replicate the geospatial data to all applications and appliances that require it. Bidders shall describe the proposed SIF along with the replication methodology that will be employed to distribute new geospatial data to appliances that require it in a timely manner.

At the heart of the GIS to ECRF/LVF integration is the DDTi Data Manager NXG solution. This function acts as the Spatial Information Function (SIF). DDTi Data Manager NXG supports the periodic loading of GIS data from external systems in "Standard" mode, or can be used in "Enterprise" mode, which provides full read/write data access to authenticated users and publishing of data edits in real-time. Because MassGIS will be maintaining GIS data in an external system and providing it periodically to the SIF, the deployment of DDTi Data Manager NXG in "Standard" mode only is proposed. The remainder of this portion of the response is written accordingly.

GIS data is uploaded to the DDTi Data Manager NXG via DDTi Data Load NXG, which features an intuitive web interface for provisioning the SIF with geospatial data. Authorized users upload data in shapefile format (other formats can be used, and the GDIT team will work with MassGIS to implement the most effective solution), verify that the data is in the expected schema, and initiate the load process into the SIF. Alternatively, automated routines can be set up to populate the SIF without having to upload via the web interface. The load into the SIF system does not do a complete overwrite; rather, it performs a change detection operation. As a result, a full historical record of all data changes can be maintained by the system, and detailed results of any load errors are provided. This process, either with the web interface or using automated routines, can be run as frequently as needed, although daily is recommended.

The following screenshot shows the DDTi Data Load NXG web interface, used to provision data to the SIF.

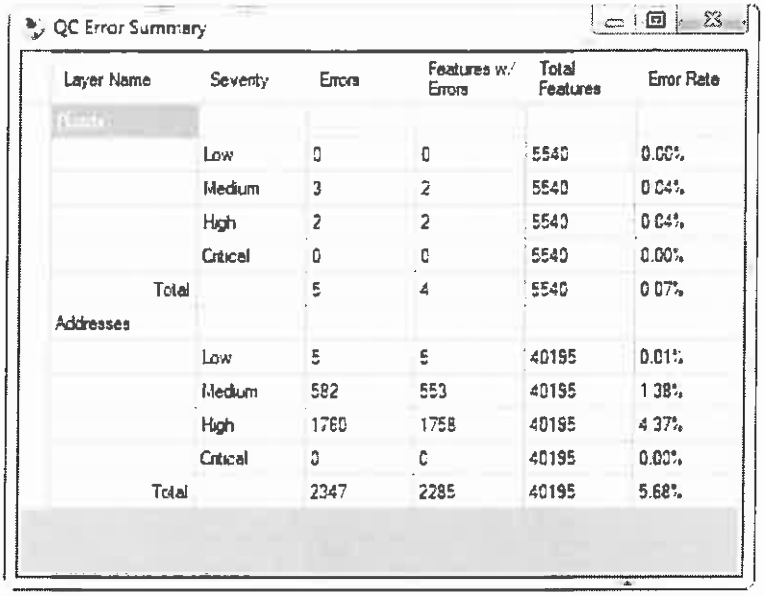


Once the data load is complete, DDTi Data Manager NXG performs numerous quality control checks on the data. The resulting QC errors can be viewed directly using the DDTi Data Manager NXG client or any software capable of consuming ESRI-based web services. This will allow MassGIS to view any map data discrepancies in real-time. The following screenshot shows the SIF's QC error layer with an ArcMap client.

Following the QC process, if the number and severity of any errors are within configurable limits, DDTi Data Manager NXG will automatically publish updated data the to the master ECRF/LVF database. This database acts as a replication master, pushing all changes using Microsoft SQL Server replication to child databases that are used for ECRF/LVF functionality.

All replication distributors run on the master database to minimize the load on the databases that are being actively used for LoST query processing. SQL Server replication occurs in near-real-time.

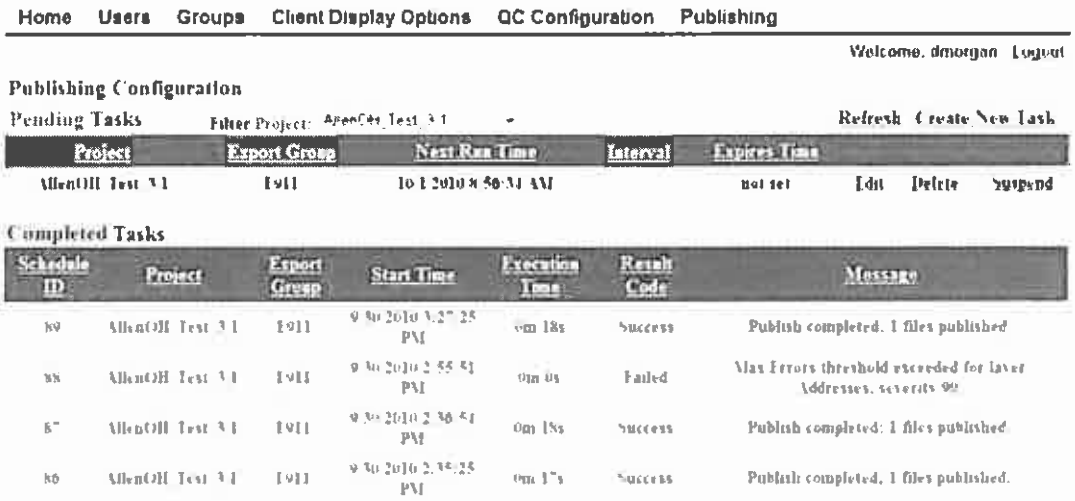
The SIF also provides reporting, allowing the Commonwealth real-time access into the state of the datasets used by the ECRF/LVF. The following screenshot shows the real-time data quality report.



QC Error Summary

Layer Name	Severity	Errors	Features w/ Errors	Total Features	Error Rate
Roads					
	Low	0	0	5540	0.00%
	Medium	3	2	5540	0.04%
	High	2	2	5540	0.04%
	Critical	0	0	5540	0.00%
Total		5	4	5540	0.07%
Addresses					
	Low	5	5	40195	0.01%
	Medium	582	553	40195	1.38%
	High	1760	1758	40195	4.37%
	Critical	0	0	40195	0.00%
Total		2347	2285	40195	5.68%

Additional publishing routines can be set up for other applications that may need the data. The next screenshot shows the Publishing configuration from the SIF's administrative web interface. This allows administrators to create publishing tasks that export copies of the data into a format that is required by third-party applications. For example, the CPE vendor may require a certain data extract that is different from what the CAD vendor requires.



Home Users Groups Client Display Options QC Configuration Publishing

Welcome, dmorgan Logout

Publishing Configuration

Pending Tasks Filter Project: AgencyCes_Test_3_1 Refresh Create New Task

Project	Export Group	Next Run Time	Interval	Expires Time			
AllenOH_Test_3_1	E911	10/1/2010 8:50:31 AM		not set	Edit	Delete	Suspend

Completed Tasks

Schedule ID	Project	Export Group	Start Time	Execution Time	Result Code	Message
89	AllenOH_Test_3_1	E911	9/30/2010 3:27:25 PM	0m 18s	Success	Publish completed. 1 files published
88	AllenOH_Test_3_1	E911	9/30/2010 2:55:31 PM	0m 0s	Failed	Max Errors threshold exceeded for layer Addresses, severity 99
87	AllenOH_Test_3_1	E911	9/30/2010 2:36:31 PM	0m 18s	Success	Publish completed. 1 files published
86	AllenOH_Test_3_1	E911	9/30/2010 2:35:25 PM	0m 17s	Success	Publish completed. 1 files published.

Geospatial Data Stored on the SIF Made Available Outside the ESInet

It is envisioned that over time, the contractor may need access to provisioned geospatial data stored on the SIF to, for example populate their own LVFs and ECRF for location validation and call routing prior to entry on the ESInet. CPE at the PSAPs (e.g., CAD systems) may also need to be provisioned with geospatial data stored on the SIF. Bidders shall describe how geospatial data stored on the SIF can be replicated or otherwise made available to entities outside the ESInet and to PSAP applications.

DDTi Data Manager NXG can be configured to publish any number of additional exports of the GIS data to Microsoft SQL Server (spatial) databases, or in shapefile or other ESRI formats. These exports can be customized to meet the data formatting requirements of the systems that will consume the data. SQL Server databases can be replicated to other SQL Server instances using built in SQL Server replication.

Figure 36 shows the data flow from GIS editors into the DDTi Data Manager NXG (SIF), and out to ECRF/LVF and other databases and consumers.

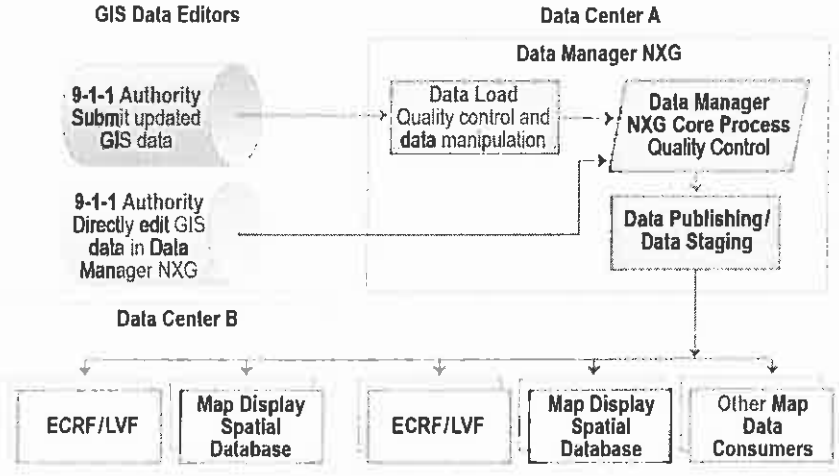


Figure 36. Logical Flow for GIS Data Updates to SIF and Related Database Instances

If the Commonwealth wishes to allow access to the data outside of the ESInet, DDTi Data Manager NXG will be configured to publish the desired data sets to the DMZ, where users can be given access to download the data.

8.7.15. Recording and Reports

The system shall have an event recorder that shall log all transactions for all payloads performed on the applications and appliances, including without limitation, 911 and administrative line voice calls, to an i3-compliant logging service. The event recorder shall log all such transactions at the data centers. The response shall describe in detail how logs may be retrieved and transferred to other media for off-site use.

The system shall log all events described within the i3 standards in accordance with such standards. Bidders shall describe in detail the length of time that the system's event recorder logs events

The GDIT team proposes Equature® from DSS, which fully supports event-logging functions specified in the Logging Service section of NENA 08-003. DSS has been actively involved as a primary contributor in defining the NENA logging and recording specifications from the initial version through NENA 08-003 v2, which is being finalized in standards. All of the logging and recording functions have been tested in NENA's ICE 8, at which DSS was the lead, providing

the chair of that event at NENA's request. DSS logging is also fully tested in GDIT's i3 Solutions Interoperability Lab. DSS is committed to maintaining conformance to the i3 standards going forward, and has participated in every ICE event to date as part of that effort. The Commonwealth is quite correct to recognize the critical nature of LogEvent data in incident reconstruction, and Equature will provide reporting and troubleshooting capabilities far beyond anything that has been available in the past. Equature's browser client, Viewpoint®, includes an easy-to-use incident reconstruction tool that allows a user to display and playback all of the multimedia activity just as it occurred. It supports the show, display, play, or mute of audio and video media, and displays textual content with the original timing to completely reconstruct call events.

GDIT's proposed solution includes the DSS Equature, supporting the full set of LogEvents specified in 08-003 v2, deployed in a redundant architecture. Version 2 is expected to be finalized in 2014. Our various ESInet partners are committed to implementing NENA standards as they evolve, including support for the version 2 format of event logs. Prior to providing v2 support, GDIT and our partners are working in the GDIT i3 Integration Lab to test and implement a suitable event logging construct that will deliver a highly functional event logging capability, although not in exactly v2 format initially.

The GDIT team proposes an Equature logging server in each data center, with each server capable of handling 100% of all Commonwealth logging traffic. NG9-1-1 elements will be configured to write LogEvents to both Logging Services simultaneously, as specified in 08-003 v2. The data center logging services will also receive LogEvents generated at the terminating PSAP to provide redundancy for those as well.

Equature includes the Viewpoint browser client for retrieving both LogEvents and Media. It includes a "Scenario Reconstruction" tool that allows the user to select the desired Media and LogEvents, and then bookmark them, save them to offline media, or zip them and email them. Equature supports all LogEvents specified in 08-003 v2, and has tested them with other vendors.

Equature will log events from the time the call hits the first element in the ESInet (usually the BCF), and continue logging until the incident is closed (and occasionally after). The administrator sets a retention policy on both events and media. When expired, old events and media are deleted (when space is needed for new ones). Calls that are marked as "protected" are not deleted until the protected flag is removed.

The Equature servers proposed provide RAID storage in each of the redundant systems sufficient to store events for a period of more than three years based on current Massachusetts call volume. Furthermore, files can be offloaded and aged in a planned manner to the storage system and offer a searchable and managed dataset in perpetuity.

GDIT understands that the Commonwealth is presently deploying DSS Equature to support local media recording from individual PSAPs. GDIT wishes to highlight that the same Equature systems that are deployed locally are being proposed to provide centralized event logging. As such, the event loggers being proposed can optionally be licensed to also record voice centrally. In this model, centralized recorder/loggers could augment local recording or support other sites in the future that do not have local recording. Furthermore, the use of a DSS event logger at the

data centers allows all DSS systems (data center and PSAP) to be managed as a single system from an administrative standpoint.

The proposed Equature system provides a comprehensive i3-compliant event logging solution. Using the Commonwealth's existing Equature local deployments and/or if the Commonwealth implements centralized recording on the Equature loggers in the future, the Commonwealth can utilize the Equature systems to provide Instant Recall Recording (IRR) on each event. As an added benefit, the CallStation CPE included in GDIT's proposed solution also provides an extremely robust and flexible IRR solution for telephone calls serviced by the Emergency CallWorks system. As with all functionality in CallStation, the IRR capabilities are provided at the application server within the data centers. Specific IRR features available through CallStation system include:

- IRR capture begins at the time the call begins ringback
- Recordings may be kept as long as desired
- Recordings are accessible from Call Detail Records in the Management Information System (MIS)
- Each recording is accessible from any location
- Recordings are backed up nightly with all configuration and data

The CallStation solution currently only records call traffic, 9-1-1 trunks, and optionally administrative lines. The system can record any number of simultaneous calls and saves all instant recordings for long-term playback. Recording storage is controlled by size quota rather than a fixed time window. The typical storage time is in excess of 90 days. Recordings are available for download in the DecisionStation MIS package and may be saved in perpetuity to the proposed storage solution, which is duplicated in each data center.

8.7.15.1. Event Reports

The system shall provide, at a minimum, the following event reports:

- *Time of payload entry through BCF;*
- *Time for each functional element to perform routing and PSAP assignment;*
- *Time of answer at PSAP, and*
- *Time of disconnect at PSAP.*

Bidders shall describe in detail the event reporting function of the system. Event reports shall record the timing of transit for each payload for purposes of diagnostics. All event reports shall, at a minimum, include the functional element being reported and the system time of such event. The State 911 Department and/or EOPSS/OTIS shall have remote access to such event reports. The system shall allow for the State 911 Department and/or EOPSS/OTIS to request ad hoc reports.

One hallmark of a federated, multi-vendor solution is that each system offers points of monitoring and visibility into traffic flow, conditions, and events, with some expected overlap of data, but also with the ability to perform deeper investigation into any one component of the solution. GDIT's proposed solution offers this exact model, with event data collected and reported in numerous forms and varying detail. GDIT augments available data from the ESInet systems with the deployment of purpose-built monitoring systems that perform packet

inspection, log collection, event polling, and/or traffic insertion to fully characterize, track, monitor, and test traffic, systems, and networks. GDIT's network and security operations construct leverages all data in systemic network and security management systems to provide aggregated and cohesive reports, live and historical reporting, and alerts. Our solution also deploys report customization tools (Crystal Reports) to enable customized reports through the extraction of data from across the environment. These reports will be posted on a web server within the data center DMZ for timely and controlled online reporting.

Specific to the event reports requested in this question, the DSS Equature system provides a single and unified event reporting capability that provides comprehensive reporting of payloads and transit times through the ESInet. The DSS Reporting Engine not only supports the identified reports, but it also provides a powerful ad hoc reporting capability that can be used to examine individual calls, overall call statistics for a given time period, given call types, positions, etc. All of these are based on the LogEvent data that tracks calls from cradle to grave. Individual event intervals, like how long a Functional Element (FE) took to respond to a request, can be reported on. The manager can set up ad hoc reports that are of interest on their personal dashboard for automatic display.

Equature fully supports the LogEvents defined in 08-003 v2. The header of each LogEvent gives the requested detail. The full detail of events, the functional elements that logged them, timing, and even identification of external elements that caused the events to be logged can be reported. Some of the new fields added in v2 include a digital signature, and IP address of some external element that responded to a query, agent, or agency, where applicable. Version 2 is expected to be finalized in 2014. Our various ESInet partners are committed to implementing NENA standards as they evolve, including support for the version 2 format of event logs. Prior to providing v2 support, GDIT and our partners are working in the GDIT i3 Solutions Interoperability Lab to test and implement a suitable event logging construct that will deliver a highly functional event logging capability, although not in exact v2 format.

Equature's Viewpoint browser client can be used from an authorized user within the ESInet, or through the restrictive DMZ interface to the Internet.

Where Equature provides NENA-compliant logging and recording with a single reporting engine, other components of our proposed solution also provide critical data that aligns, supports, or augments with the event reporting. Two critical examples of this include:

- Emergency CallWorks CallStation system provides a comprehensive management and statistical reporting system to provide the PSAP management personnel with real-time and historical information. The reporting system is customizable and capable of generating reports for varying time periods. 9-1-1 Call Detail Reports include ANI, ALI, seizure time, position answered, answer time, transfer time, disconnect time, and incoming trunk number. The system ships with all reports requested.

- CallStation uses a unified database back end for all captured data. This includes standard Call Detail Record (CDR) data, as well as other data such as Telecommunications Device for the Deaf (TDD) conversations, user added notes, etc. MIS reports and dashboards gather data directly from this online database and therefore have access to real-time data as it is updated. Furthermore, the system provides a dashboard that specifically displays

and allows summary and detailed exploration of active calls. The complete database is dumped to a file nightly for safekeeping. Data is available to the user in a referential hyper-linked format which may be browsed at the user's leisure. This allows the user to begin with the data they know, such as trunk, and drill down and/or horizontally toward the data they need. All data views may be filtered based on a wide variety of variables including user(s), group(s), trunk(s), date(s), time, etc. Selected report examples from CallStation are provided below.

Calls by Line Type

ECX Test Network #1

Start Date 2013-09-01 Shift Start 08:00

End Date 2013-09-30 Shift End 18:00

Operator Groups main, remote1, remote2, remote3

	9-1-1	7-Digit Emergency	Admin	Total
Calls Presented	455	1	0	456
Answer Time - Average	00:28.0	00:05.0	00:00.0	00:25.9
Answer Time - Median	00:05.0	00:05.0	00:00.0	00:05.0
Answer Time - Maximum	23:42.0	00:05.0	00:00.0	23:42.0
Calls Abandoned	205	0	0	205
% Abandoned	45.05%	0.00%	0.00%	44.96%
Calls Answered	250	1	0	251
Agency Goal	95% - 10SEC	90% - 10SEC	80% - 10SEC	
Within Goal	168	1	0	169
% Within Goal	67.20%	100.00%	0.00%	67.33%
Longer Than Goal	82	0	0	82
Average Call Duration	04:48.2	01:11.0	00:00.0	04:47.3

Wed, 23 Oct 2013 09:43:4[illegible] DS072 Page 1 of 1

Figure 37. CallStation – Calls by Line Report

Calls by Position

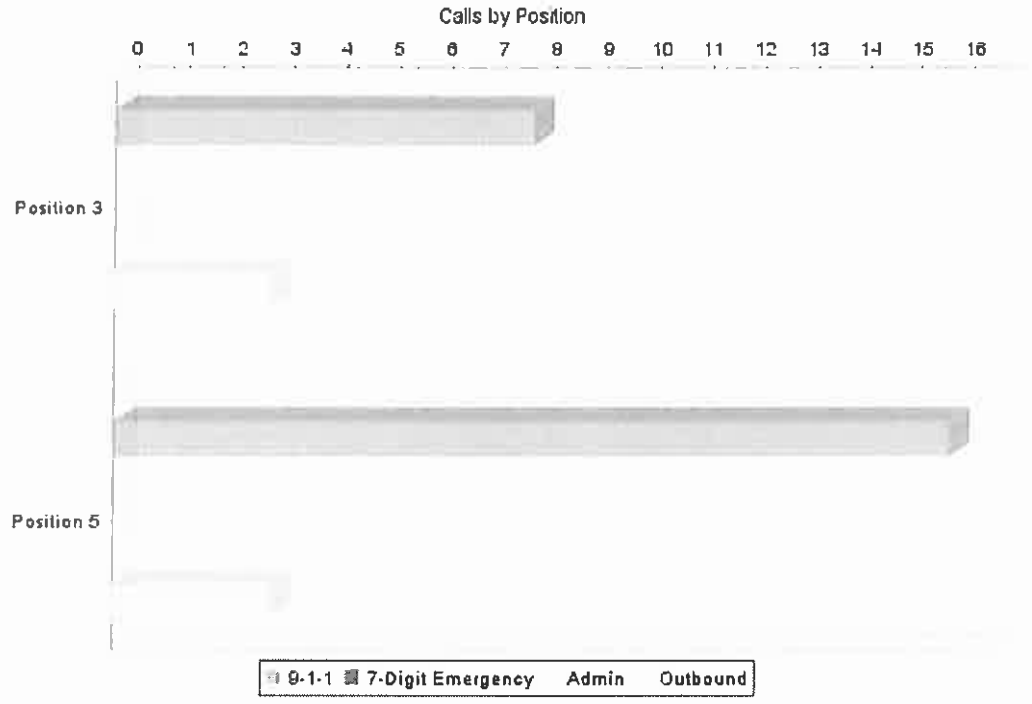
ECX Test Network #1

Start Date 2013-08-01 Start Stop –

End Date 2013-08-31 End Stop –

Position Groups –

Position	9-1-1	7-Digit Emergency	Admin	Outbound
3	8	0	0	3
5	16	0	0	3
Total	24	0	0	6



Tue, 3 Sep 2013 10:36:34 DS072 Page 8 of 8

Figure 38. CallStation – Calls by Position Report

Calls Answered Within 10 Seconds

ECX Test Network #1

Start Date 2013-10-01 Shift Start 08:00

End Date 2013-11-01 Shift End 18:00

Dispatch Groups: main, remote1, remote2, remote3

	9-1-1	7-Digit Emergency	Admin
Answered Within 10 Seconds	84.66%	0.00%	86.67%
Average Answer Time	00:03.7	00:00.00	00:03.8
Median Answer Time	00:03.0	00:00.00	00:04.0
Average Call Duration	06:46.8	00:00.00	01:13.5
Median Call Duration	01:17.0	00:00.00	00:28.0

Mon, 4 Nov 2013 14:15:49 CS372 Page 1 of 1

Figure 39. CallStation – Calls by Answer Time Report

Calls by Hour and Day

ECX Test Network #1

Start Date 2013-10-01

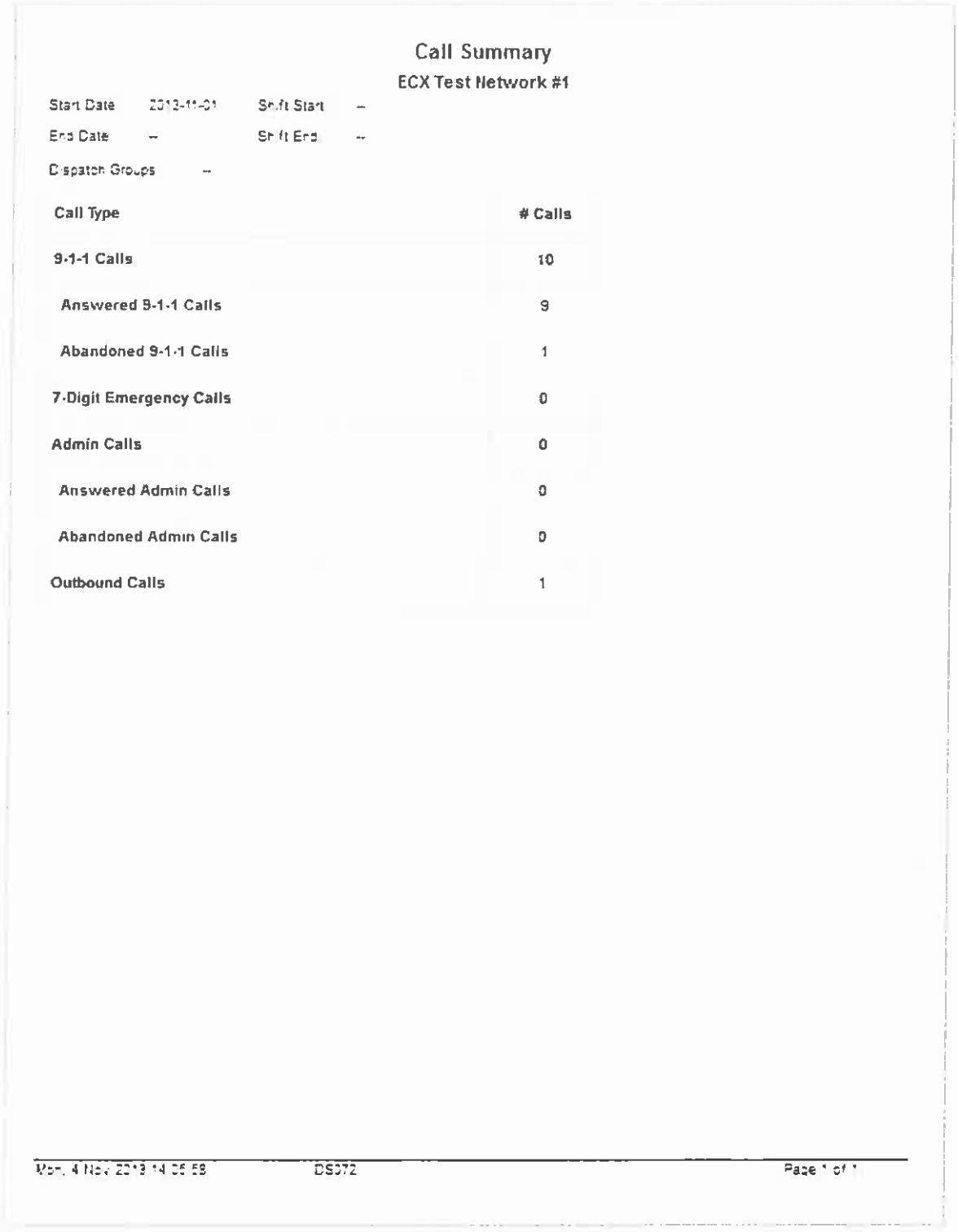
End Date 2013-11-01

Queues –

Hour	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Total	% Total	Avg	Med
00:00 - 01:00	0	0	0	0	0	0	0	0	0.00%	0	0
01:00 - 02:00	0	0	0	0	0	0	0	0	0.00%	0	0
02:00 - 03:00	0	0	0	0	0	0	0	0	0.00%	0	0
03:00 - 04:00	0	0	0	0	0	0	0	0	0.00%	0	0
04:00 - 05:00	0	0	0	0	0	0	0	0	0.00%	0	0
05:00 - 06:00	0	0	0	0	0	0	0	0	0.00%	0	0
06:00 - 07:00	0	0	0	0	0	0	0	0	0.00%	0	0
07:00 - 08:00	0	0	0	0	0	0	0	0	0.00%	0	0
08:00 - 09:00	0	0	21	2	6	9	0	38	0.41%	5	2
09:00 - 10:00	0	3	38	1,853	7	11	0	1,910	20.39%	272	7
10:00 - 11:00	0	8	8	11	9	2	0	38	0.41%	5	8
11:00 - 12:00	0	2	8	9	17	1	0	37	0.39%	5	2
12:00 - 13:00	0	0	5	4	6	4	0	19	0.20%	3	4
13:00 - 14:00	0	4	2	10	2	3	0	21	0.22%	3	2
14:00 - 15:00	0	27	8	11	1,009	36	0	1,091	11.64%	156	11
15:00 - 16:00	0	11	6	11	9	895	0	932	9.95%	133	9
16:00 - 17:00	0	18	928	18	3,201	871	0	5,036	53.75%	719	18
17:00 - 18:00	0	1	220	12	10	4	0	247	2.64%	35	4
18:00 - 19:00	0	0	0	0	0	0	0	0	0.00%	0	0
19:00 - 20:00	0	0	0	0	0	0	0	0	0.00%	0	0
20:00 - 21:00	0	0	0	0	0	0	0	0	0.00%	0	0
21:00 - 22:00	0	0	0	0	0	0	0	0	0.00%	0	0
22:00 - 23:00	0	0	0	0	0	0	0	0	0.00%	0	0
23:00 - 24:00	0	0	0	0	0	0	0	0	0.00%	0	0
Total	0	74	1,242	1,941	4,276	1,836	0	9,369			
% Total	0.00%	0.79%	13.26%	20.72%	45.64%	19.60%	0.00%				
Average	0	3	52	81	178	76	0				
Median	0	0	0	0	0	0	0				

Wed, 6 Nov 2013 09:22:54 DS272 Page 1 of 1

Figure 40. CallStation – Calls by Hour and Day Report



Call Summary

ECX Test Network #1

Start Date 2013-11-01 Shift Start --

End Date -- Shift End --

Dispatch Groups --

Call Type	# Calls
9-1-1 Calls	10
Answered 9-1-1 Calls	9
Abandoned 9-1-1 Calls	1
7-Digit Emergency Calls	0
Admin Calls	0
Answered Admin Calls	0
Abandoned Admin Calls	0
Outbound Calls	1

Mon, 4 Nov 2013 14:05:58 DS372 Page 1 of 1

Figure 41. CallStation – Calls Summary Report

Included in our proposal is the Oracle Palladion monitoring system, which is provided to perform packet inspection on all services, and generates measurements on media QoS and associated signal control messages between ESInet systems. Palladion provides detailed packet-level analysis of all calls in real-time and maintains a persistent historical and searchable database. Such real-time monitoring is a critical component of the IP-based reliability model necessary for proactive maintenance activities. But further, this actual data derived for packet inspection allows reporting to the packet level, correlated to a specific event. A searched call for example will provide detailed information on the signaling between components that enabled the call to be setup, any in call signaling (e.g., conferencing or transfer), the packets' performance during the call, and much more. All information would be timestamped to correlate to reports from other systems, such as DSS Equature. Further, Palladion will aggregate individual call information to allow reporting of Call Detail Records (CDR), Key Performance Indicators (KPI), network tracing, and log reporting. Palladion's capabilities are not limited to only ESInet components; they include any device involved in the call flow, to include firewalls and networking. Below are selected Oracle Palladion reports.

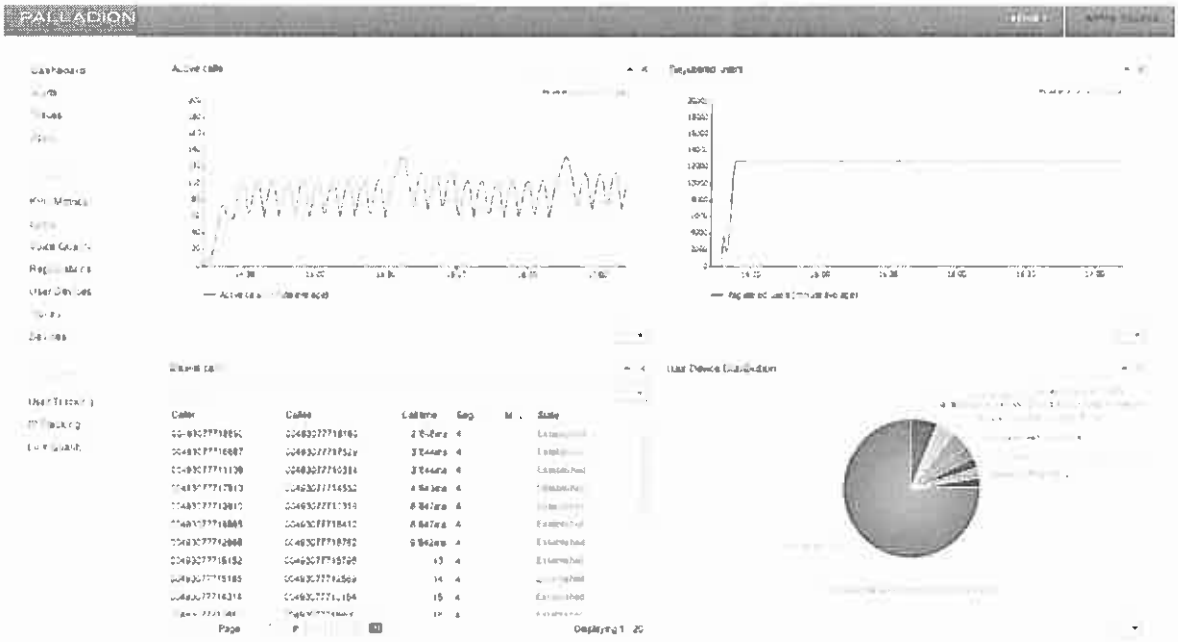


Figure 42. Oracle Palladion Dashboard

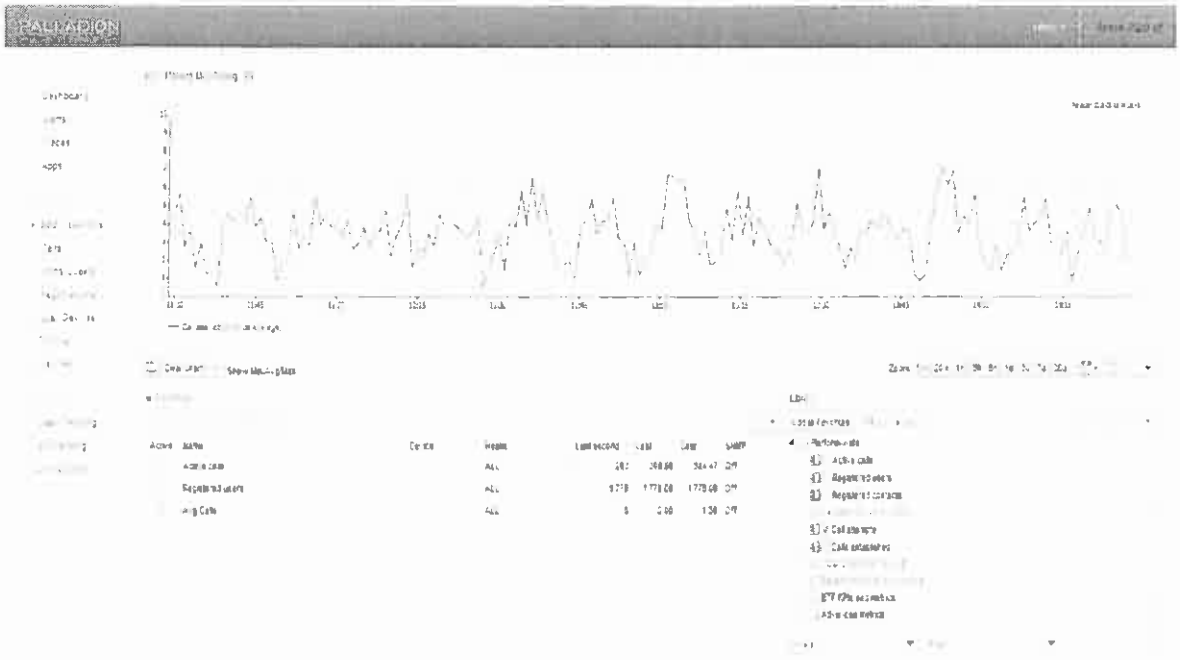


Figure 43. Oracle Palladion – KPI and Metrics Report

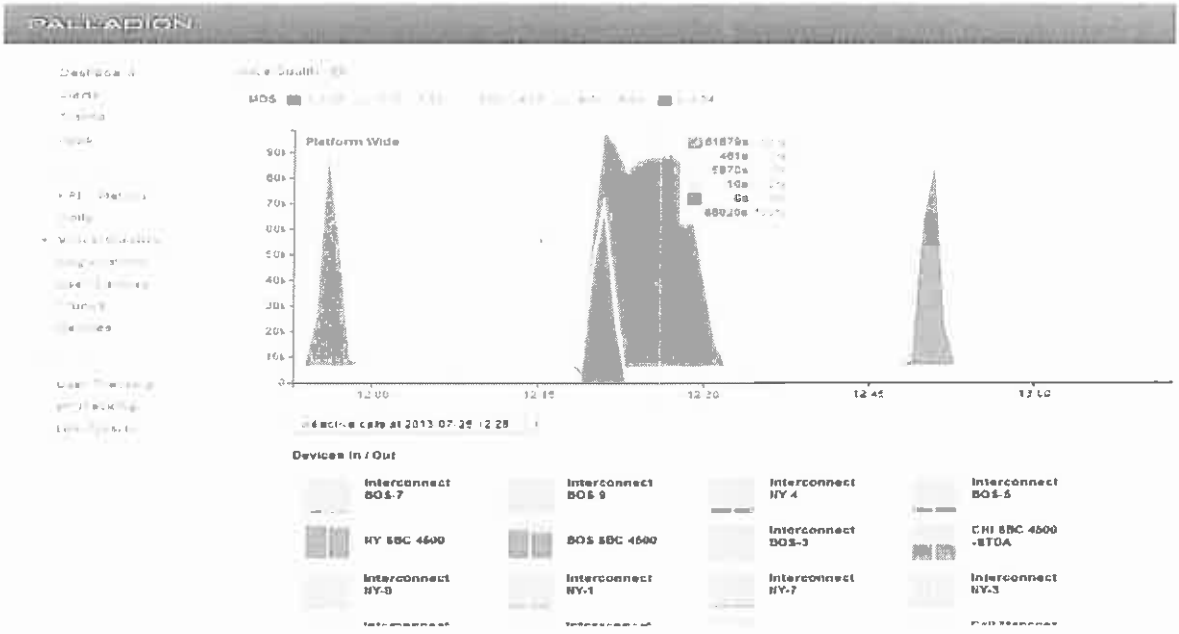


Figure 44. Oracle Palladion – Voice Quality Report

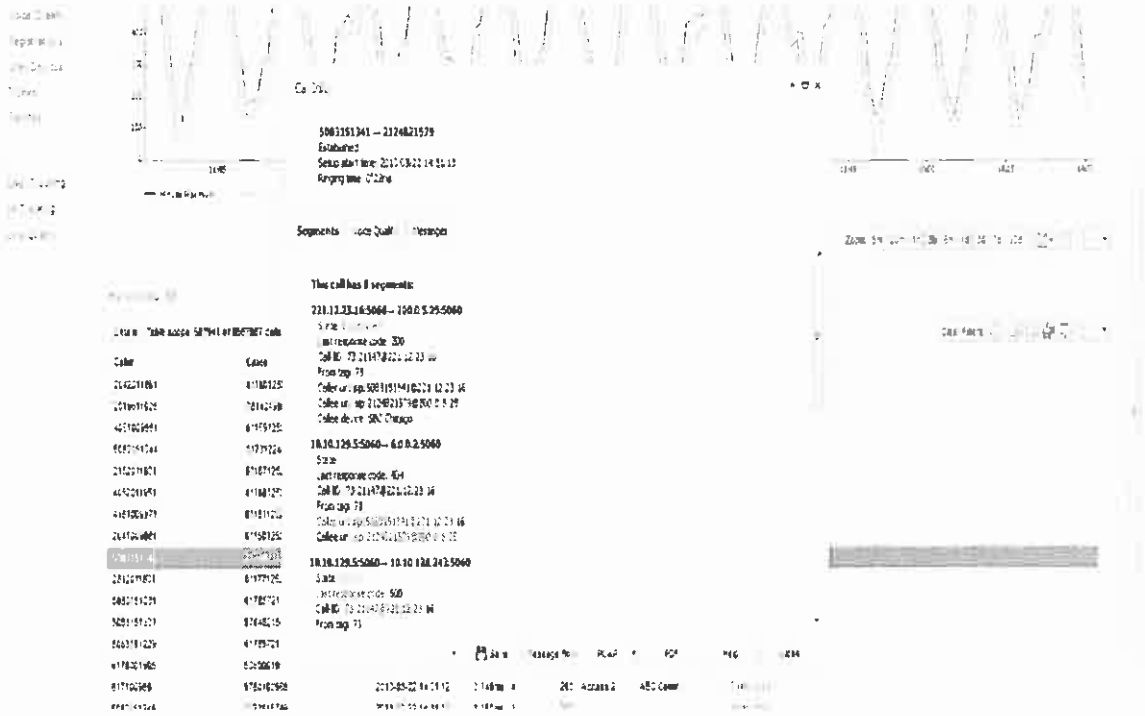


Figure 45. Oracle Palladion – Individual Call Drill Down Report

8.7.16. Printers

The system shall interface with and shall include one (1) printer at each PSAP to be used as a system printer. The contractor shall maintain, effective as of the date of the cutover of the PSAP to the Next Generation 911 system, the existing printers located at PSAPs. The types of existing printers located at PSAPs are HP P2035 LaserJet and HP Pro 400 LaserJet. In addition, bidders shall propose, with optional pricing, replacement printers to be used as a system printer at PSAPs. The replacement printers shall be of equivalent specifications as those currently located at PSAPs. The contractor may, upon the request of the State 911 Department, be required to add a secure LAN interconnection at a PSAP for the purposes of sharing an existing PSAP printer, with the pricing to be negotiated by the parties.

A network printer is provided in the GDIT solution at every PSAP and remote location, including at the Limited Secondary PSAPs. Access to network printers will be established at workstations as part of the group policy.

Network printing places high demands on a router, demanding availability of host memory and, if not implemented correctly, affecting router services. With this consideration, GDIT has selected an enterprise-grade router at even the smallest locations.

Please see optional pricing for replacement printers to be used as system printers at PSAPs.

8.7.17. Instant Recall Recorders

The system shall include the ability for individual call taker workstations to instantly replay prior payloads or payloads in progress, regardless of the payload type or size. The install recall recorder shall allow, at a minimum, replay time of sixty (60) minutes for voice calls and the equivalent of sixty (60) minutes, in size, for other payload types. The response shall describe how the system addresses this issue, including the amount of available recording time and/or extended memory requirements for each type of payload (i.e., voice, text, photographs, video, telematics, etc.) The response shall describe whether the system has the ability to replay graphics.

The CallStation CPE proposed in the GDIT solution includes an integrated Instant Recall Recording (IRR) solution for telephone calls. As with all functionality in the Emergency CallWorks CallStation system, the IRR capabilities are provided at the Application Server located at each data center, which is fully integrated into the call taker workstation with point-and-click access and operation. Additional capabilities include:

- IRR capture begins at the time the call begins ringback
- Recordings may be kept as long as desired
- Recordings are accessible from Call Detail Records in MIS
- Each recording is accessible from any location
- Recordings are backed up nightly with all configuration and data

The CallStation system currently only records voice traffic associated with 9-1-1 and those administrative lines used within the CPE. The system can record any number of simultaneous calls and saves all instant recordings for long-term playback. Recording storage is controlled by size quota rather than a fixed time window. GDIT's proposed solution provides in excess of 90 days (not minutes) of recall storage accessible by all call taker positions, based on typical call volume and duration. Recordings are available for download in the DecisionStation MIS package and may be saved indefinitely by downloading them to a storage system.

The Commonwealth presently utilizes DSS Equature® at many locations. GDIT has provided Equature as a centralized event logger with the option of adding central voice recording. Using either the local recorder (for local traffic) or the central recorder (option), Equature also supports an i3 conformant Instant Recall Recorder (IRR) capability that is capable of being used at call taker workstations. The Equature IRR client tool is part of the Viewpoint browser client. The Administrator configures what an Agent sees in the tool, and what they can do with it. For example, they can see only their calls (and radio channels), going back only 60 minutes, etc. What an Agent can see and do in Viewpoint is completely configurable, allowing for maximum flexibility with appropriate security.

Since Equature is constantly recording all media, it is available for Instant Recall as soon as it has been received. Memory and storage requirements are therefore placed on the Equature server, and not on the workstation. The only workstation requirements would be for minimal caching or buffering of data or media during display or playback. The bandwidth required to deliver media from Equature to the workstation for recall is the same as for delivering across the network for call handling – about 100k for audio and about 300k for video. Processor resources on the workstation to handle these media are also identical to that required for handling the same media in the call itself. Bandwidth and processor resources to handle textual content are miniscule by comparison, and are considered to be "in the overhead."

08-003 has never provided standardized mechanisms for handling picture data specifically. However, picture data can be delivered in an MSRP session, and an MMS message will presumably be transcoded to MSRP in the future. It is also possible to send picture data within an established SIP session by other means. So picture data can be expected. Equature supports display of picture data (and common document types as well) within Viewpoint, so we expect that displaying picture data in the IRR or replay functions will be doable when standard mechanisms have been clarified, and DSS intends to conform to those standards when they are developed.

8.7.18. Digital Logging Recorders

The system shall have two (2) interfaces to the Next Generation 911-capable DLRs furnished to PSAPs by the State 911 Department and currently in use at PSAPs. The system shall integrate the existing DLRs into the LAN through an IP connection (and not through an analog connection). The State 911 Department expects to add VoIP cards to the DLRs furnished by the State 911 Department and currently in use (through another procurement mechanism outside the scope of this RFR). The contractor shall provide a mounting solution adjacent to or within the same cabinet or rack that houses the Next Generation 911 CPE for the existing DLRs and for any and all new DLRs, whether supplied by the contractor at the request of the State 911 Department or otherwise.

At the request of the State 911 Department, the contractor shall provide, equip, install, and maintain new digital logging recorders that are fully i3 compliant.

The CallStation CPE proposed in the GDIT solution can provide IP and analog voice access for recording purposes and also supports output of ALI and answering position details to logging recorders. The Emergency CallWorks system provides a great deal of flexibility in supporting multiple and remote recording interfaces.

The GDIT team proposes the DSS Equature platform to provide NENA-compliant event logging service functionality specified in NENA 08-003. GDIT is also proposing media recording as an optional component of the event logging, with the ability to record all NG9-1-1 calls and CPE-based administrative lines and media centrally. In the proposed redundant data center design, the failure of a single data center's logging service will be fully survived by the other data center. If an entire data center is down, the other data center processes calls and records media to its own logging service.

This option includes storage for a minimum of two weeks – long enough to recover data in the event of a recording problem. This design approach is the most cost-effective method of achieving the high-availability goals the RFR has specified. As a core service (ref. NENA 08-003), the logging service must meet the 99.999% availability requirement of the RFR, and it is impossible to achieve that goal without redundancy. The proposed option of providing redundancy via share logging services in the data centers is by far the least expensive way of meeting the availability requirement, and the option proposed conforms to the current recommendations in NENA 08-003 v2.

The proposed recording availability architecture provides geo-diverse logging service instances that simultaneously log and record all events and media, and that support a workable failover scheme, thereby meeting the 99.999% availability requirement.

In the absence of guidance from NENA, retention policy for redundantly recorded media must be considered. Equature provides a retention policy feature that should be used to set the period that recorded media must be retained. The media is automatically deleted when that period has expired. NENA does not provide guidance on retention of redundant copies of media. These copies should be considered "failsafe" copies, rather than backup copies – the intent is for the PSAP to download this media only in the event that some failure precluded their own logging service from recording it. The Commonwealth should decide what is a reasonable retention period (e.g., two weeks) and publish the policy to all the PSAPs so that they understand that the media is only for the purpose of recovery during that period. The Department should consider retention policy for LogEvents also – it may want to retain these longer, since they have value for troubleshooting and statistical reporting beyond their use as call media-related metadata. Since all records are discoverable, having a published policy and an automatic retention policy function that enforces it should provide the Department and its PSAPs with a clearly

understandable mechanism that governs the management of these temporary failsafe records – while providing the required redundancy to meet the 99.999% availability requirement.

The Equature product is fully i3-compliant and supports the Session Recording Protocol (SIPREC) for recording media, as specified in 08-003 v2 for NG9-1-1 payloads of audio, video, real-time text, and Message Session Relay Protocol. Other text content like sensor alarms and vehicle Automatic Crash Notification data that is delivered in a Common Alerting Protocol (CAP) message is logged via a "LogEvent," per 08-003. Equature supports all of these media types, and the interfaces have been tested against multiple vendors. Administrative lines that are SIP based are supported through the same interface. Analog or legacy digital administrative lines require line cards (available, but not quoted). SIPREC is the active recording protocol specified for media recording in NENA 08-003 version 2 (soon to be released). Specific functional elements are required to support sending media to the logging service (e.g., Equature) via the SIPREC interface. Any functional element that has media may send media, but call handling, BCF, gateways, and bridging functional elements must support it. We believe the proposed solution accomplishes this in the most effective (and cost-effective) way. DSS has participated in every NENA ICE event in order to continuously test logging service interfaces as the standards have developed, and DSS provided the chair for the recent ICE 8 event that tested the logging and recording interfaces.

The proposed option for full media recording in the data center logging services is not just highly recommended – it is clearly required to get anywhere near the availability goal stated in the RFR. With all media being recorded at the PSAP, and also at the serving data center, any problem at either end will not result in a loss of service or data. This option provides very high availability at the lowest possible cost.

Equature provides the SIPREC media/metadata recording interface required by the i3 document, 08-003 v2. This interface is available to both PSAP elements and ESInet core services elements, and works equally well with both.

A mounting solution will be provided for DLR as required.

8.7.18.1. Local Logging Recorder Interface

The system shall provide a local recorder interface for 911 audio on a per position basis. The system shall provide the ability to interface with both analog and digital logging recorders.

The system shall provide the capability to optionally generate an outward "beep" tone on selected audio call sources at fifteen (15) second intervals.

The CallStation system can provide either IP and/or analog voice access for recording purposes at every local PSAP, on a per-position basis. The system also supports output of ALI and answering position details to logging recorders and provides a great deal of flexibility in supporting multiple and remote recording interfaces. Insertion of 'beep' tone is not presently supported.

The proposed DSS Equature logging and recording platform supports both analog and digital interfaces. The NG9-1-1 media recording and event logging interfaces are all IP; therefore, that will be the primary interface to Equature. However, digital and analog interfaces can be retained or added as necessary according to a PSAP's need.

The existing Equature system has the beep tone capability on analog input channels. For IP channels, it is best for the Session Recording Client (SRC) – the element that is sending media to the recorder, to send the beep tone. SRCs are typically Back to Back User Agents, and can generate an outgoing-only tone with the appropriate characteristics.

8.7.19. Voice Quality Standards

The Mean Opinion Score, or MOS, provides a numerical indication of the perceived quality of received media after compression and/or transmission. The system shall obtain a MOS of four (4) or higher per the numerical measure set forth in the table below. Bidders shall describe in detail the methodology to be used to meet this target and provide ongoing measurement to ensure voice quality.

MOS	*Quality*	*Impairment*
5	*Excellent*	*Imperceptible*
4	*Good*	*Perceptible but not annoying*
3	*Fair*	*Slightly annoying*
2	*Poor*	*Annoying*
1	*Bad*	*Very annoying*

Mean Opinion Score (MOS) is a traditional measure of voice quality, originating from a process of using human evaluators to rate sound quality. 'Carrier' quality was defined as having a MOS of 4.0 or higher. In the modern context, MOS is rated using one of two techniques: calculated and measured.

In a calculated method, systems report on the transit performance of packets (packet loss, jitter, and delay) at intervals within a call, and these measures are used in a calculation of MOS. This method does not consider several factors that are unrelated to the three packet performance measurements (packet loss, jitter, and delay), including echo and volume. Furthermore, the interval measurements are often average measurements (over time) that are absolutely helpful and indicative of overall quality, but also may not always accurately reflect instantaneous problems, thereby hiding short durations of poor quality over a long time interval.

By far, the most accurate and meaningful method for determining MOS (short of human hearing) is to capture and measure actual voice media streams. GDIT's proposed solution allows for both methods, utilizing information from systems to continuously report on KPIs (like packet performance). Further, GDIT's proposed solution deploys the Oracle Palladion monitoring system, with probes placed at each PSAP to capture information as it ingresses and egresses the network.

Finally, SLAs are key quality performance mechanisms that allow the network to be monitored and subcontracted in key domains. By establishing SLAs across domain boundaries, each domain contractor/owner can be monitored for contractual performance, and defects can be isolated by domain. In this way, end-to-end performance becomes a composite of the identified administrative domains, to include WAN core, access Loops, PSAP network data center network and egress traffic.

GDIT's proposed solution provides a holistic approach to delivering QoS using all defined mechanisms, with reporting to demonstrate historical performance. GDIT's proposed solution will deliver an average MOS of 4.0.

8.7.20. Back to Back User Agent Usage

If SIP or RTP traffic needs to cross boundaries, it shall be handled with back to back user agent, or B2BUA, type of session border controllers rather than via NAT. B2BUAs shall also be used to transport SIP and RTP between IPv6 and IPv4 networks, if required.

The Oracle SBC operates as an edge proxy and SIP B2BUA. SIP sessions terminate and re-originate as new sessions route through the SBC. Network Address and Port Translation (NAPT) translations are established for each session and the Service Delivery Platform (SDP) gets rewritten forcing all session-related media to be routed through the SBC. To prevent transmission of any protected IP addresses and route information to external peers, the SBC generates new Call-ID values and modifies SIP headers. The Oracle SBC supports multiple SIP interfaces that are associated with a set of media ports thus appearing as multiple virtual SIP gateways. To route between connected networks we utilize route policies. The Oracle SBC also supports B2BUA for IPv6 to IPv4 SIP interworking.

8.7.21. Time Server

The system shall include a network time protocol service for time-of-day information. The system shall have a redundant time source located at each data center, and a time source at each PSAP. The time server shall meet time accuracy within 20.0 ms of true time. The time server shall provide additional Ethernet ports for the purposes of providing time synchronization to non-interconnected LANs. Bidders shall describe how the applications and appliances, CPE, and DLRs shall be synchronized with this time source using standards-based protocols. The contractor shall, at the direction of the State 911 Department, configure the time source at the PSAP, at the time of installation of the time source, to provide time synchronization to non-interconnected LANs.

GDIT will Engineer, Furnish, Install, and Test (EFI&T) and make operational Spectracom Netclock Time Server Model 9483s to provide Network Time Protocol (NTP) service for time of day information at the data centers and PSAPs. Each data center includes redundant time server configurations with each PSAP designed with a single time server.

The 9483 configuration includes:

- A one (1) Rack Unit (RU) chassis equipped with four total 10/100/1000 Ethernet ports. One port will be used to provide NTP for NG9-1-1 assets. The additional Fast Ethernet ports are available to provide NTP for non-interconnected LANs. The chassis is also equipped with one RS-232 port for connectivity to legacy CAD systems at the PSAPs and one Inter-Range Instrumentation Group (IRIG) port for connection to the local voice recorder.
- External Global Positioning System (GPS) antenna
- GPS antenna surge protector and grounding kit to protect the antenna from lightning strikes. GDIT will Engineer, Furnish, and Install (EF&I) ground cabling and a ground rod to properly ground the surge protector.

Timing for applications/appliances, CPE, and digital logging recorders will be derived as follows:

- All Windows-based appliances and applications will derive NTP from the network's Domain Controller. The Domain Controller itself will be pointed to the local 9483 time server across the LAN. NTP delivery is accomplished using User Datagram Protocol (UDP) on port 123.

- All LAN and router equipment will be pointed directly to the local 9483. NTP delivery is accomplished across the LAN using UDP on port 123.
- DLRs will derive NTP via a direct connection between the 9483 and the DLR.
- Legacy CAD systems will obtain NTP via a direction connection between the 9483 and the CAD system.

The proposed 9483 system meets the time accuracy requirements of with 20.0 ms of true time. GDIT, at the direction of the State 911 Department, will configure the PSAP 9483 time servers to provide NTP to non-interconnected LANs. It is assumed that this effort will take place at the time the 9483 time server is installed at the PSAP.

8.7.22. User Interface

The response shall describe in detail and shall provide specific examples and graphical depictions of the user interface, or human machine interface, specifications and shall describe in detail the flexibility and functionality of the human machine interface. The State 911 Department shall have the ability to customize the user interface.

The Emergency CallWorks user interface makes handling wireless calls easier with tightly integrated mapping, and makes handling next generation calls possible by including support for alternate call and media types. Today nearly 80% of 9-1-1 calls are wireless, and this makes it critical to have pre-answer plotting and map-based call control. Pre-answer mapping allows useful Selective Answering and queue management based on the location of the incoming Calls.

The Emergency CallWorks solution helps to speed up call handling while reducing human errors by simplifying and automating common, repetitive, and error-prone tasks. User mental context is maintained by elimination of confusing constructs such as pop-up windows. Common tasks such as transfers are partially automated using a "destination-based" design and provide the system with the context awareness to provide appropriate transfer routing and signaling depending on the type and state of the call. Callbacks are greatly simplified by providing the intelligence to perform single-click callbacks for any type of call, including wireless and long-distance calls.

The Emergency CallWorks user interface was designed from the ground up for modern call handling, including wireless and next generation calls. The system includes all standard 9-1-1 CPE functionality such as directory, call logs and history, TDD interface, single-click transfers, etc. Additionally, the system includes a tightly integrated mapping interface to facilitate a map-oriented workflow. The system also includes optional dispatching capability and user controls.

The user interface is customizable by Emergency CallWorks for some format and graphical presentation elements, including colors and function placement. This customization is achieved as a global change, and customization options can be provided to the Commonwealth under the initial implementation. Subsequent customization will require a professional services engagement.

Selected captures and explanations of the user interface are provided below (Figure 46 through Figure 52).

The CallStation user interfaces leverage a Mozilla browser, providing little to no management of a heavy user interface. This construct supports easy management, updates, and support for

remote users. The user interface provides comprehensive management of all call taker applications, including call management, Mapped ALI, and VoIP.

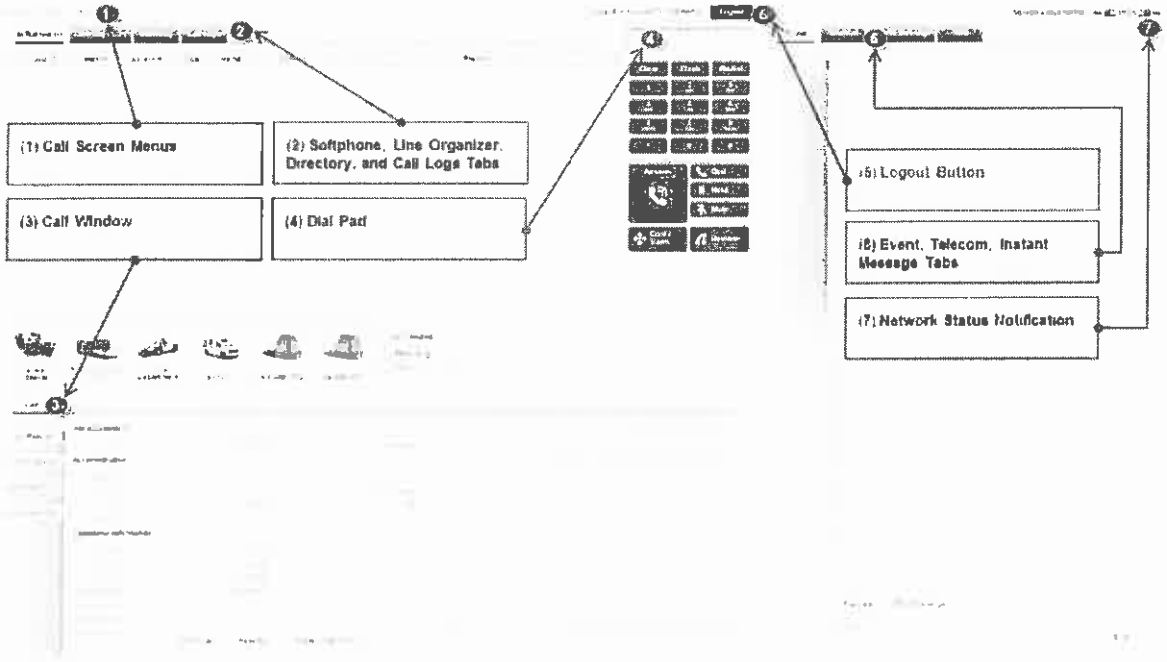


Figure 46. Layout of CallStation User Interface

The following are displayed in the CallStation Line Organizer (Figure 47):

- **Line Type Sub-Tab:** Categories such as E9-1-1, E7digit, Admin, Virtual SIP lines.
- **Status Lights:** Color indicates call state: Ringing (Red), Connected (Green), Abandoned (Blue), On-Hold (Yellow), Transferred (Black).
- **Line Table:** Displays the phone lines, active and idle. Provides full call management.

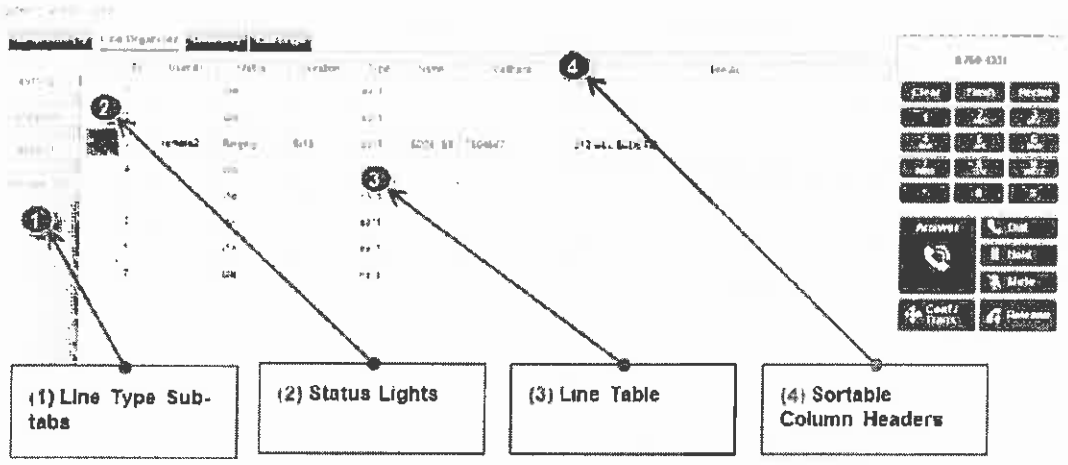


Figure 47. CallStation Line Organizer

The Directory contains all contacts configured in the system and serves an important role in transferring and creating conference calls. Entries are classified by Entry Types such as EMS, Law Enforcement, Fire, etc. Use the Dial Buttons and Directory Buttons to speed dial or transfer calls to the corresponding entries.

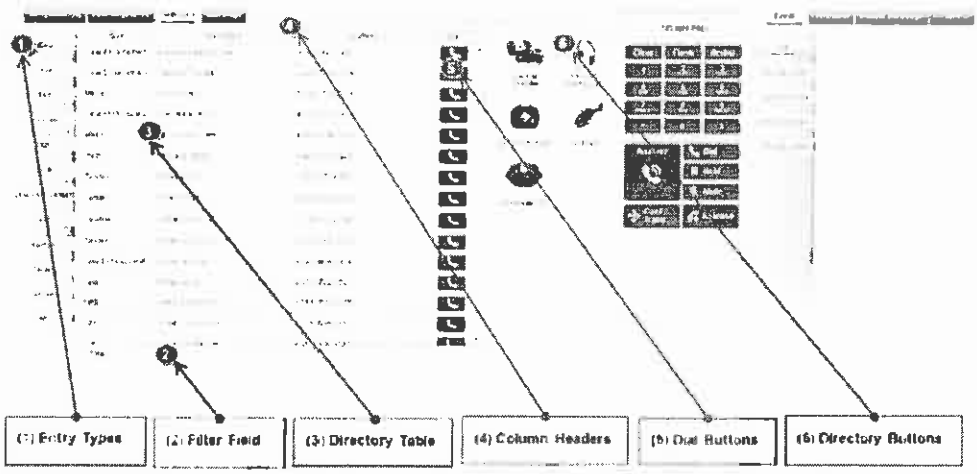


Figure 48. CallStation Directory

The CallStation Call Logs screen displays:

- **Call Types:** Call categorized by inbound and outbound.
- **Call Logs Table:** Displays call history for past 24 hours. Right-click on call to review, playback, or redial.

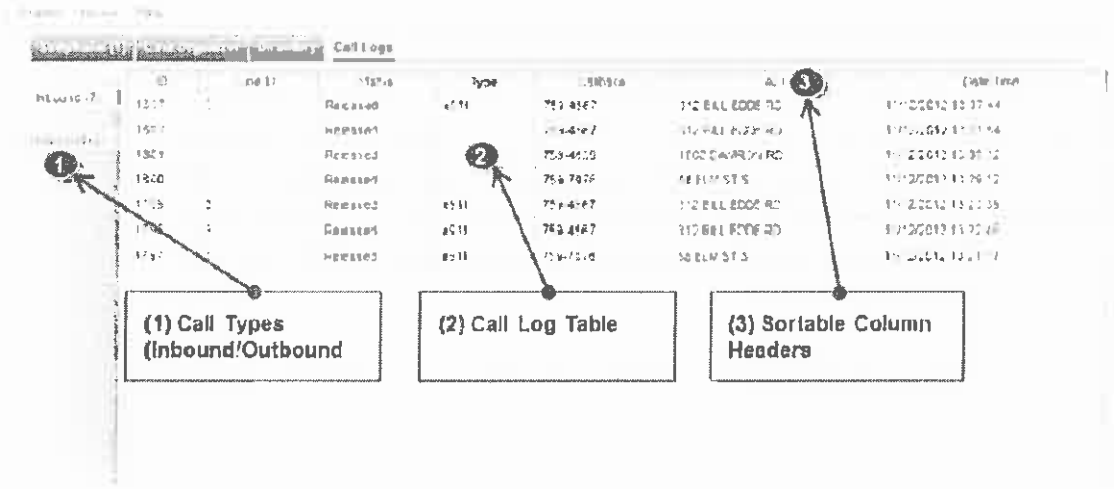


Figure 49. CallStation Call Logs

Figure 50. CallStation Call Window ALI Results

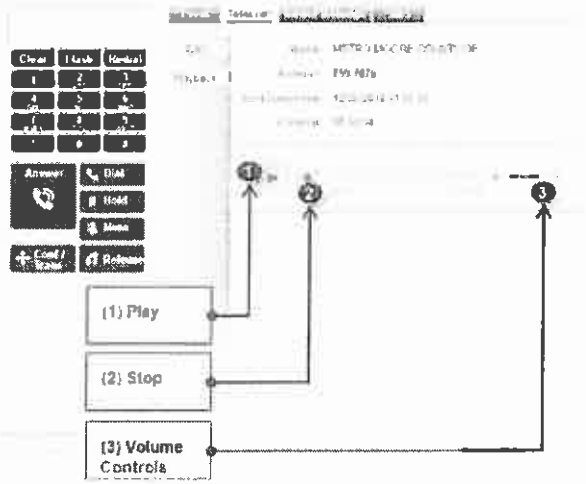


Figure 51. CallStation Call Playback

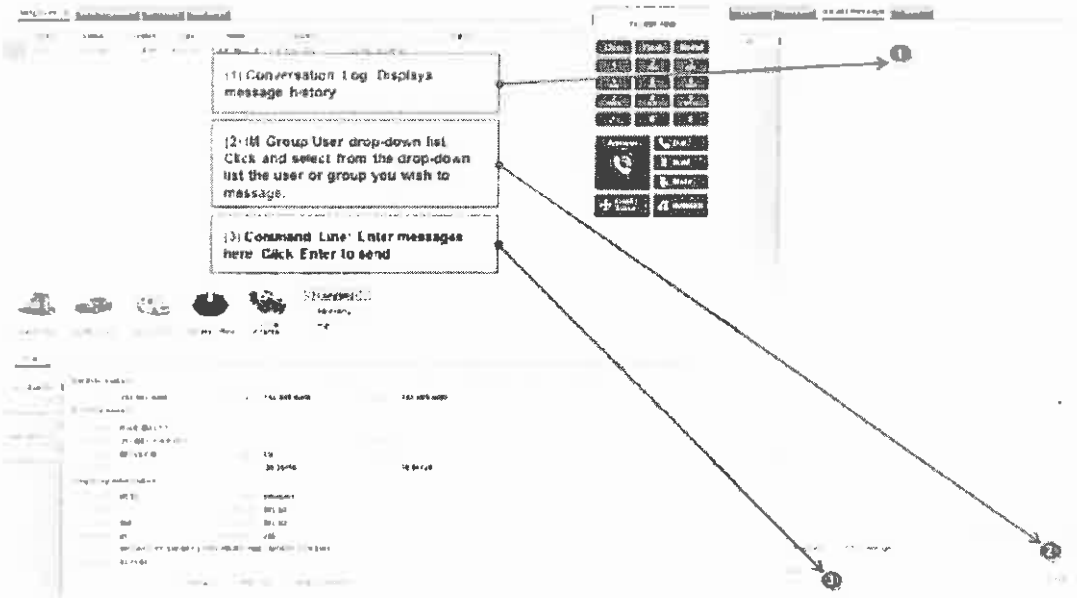


Figure 52. CallStation Instant Messaging and TDD Message Tab

8.7.23. Mapping

The response shall describe the system's mapping display functionalities and requirements for GIS data. The response shall address phase II wireless calls and shall also reflect the entire spectrum of potential payloads available within the system. The mapping display shall utilize the same geospatial data provisioned to the SIF. Mechanisms exist in i3 to replicate the data to the CPE and to its map display. Bidders shall describe how the system utilizes data replication to provision the map display available with the CPE. The system shall include a centralized map management function for mapping updates so that mapping shall be managed and distributed from a centralized location. The mapping system shall be able to interface with and utilize various interfaces, including free mapping services such as Google as well as other applications such as Pictometry. Bidders shall include the optional API for developers to create custom applications as necessary. The system shall be compatible with the most current version of ESRI software, and the response shall describe the process for staying current new releases. The map display shall allow for simple point and click functionality to obtain geodetic values of any location in the

map, to be displayed in both degrees, minute, seconds and decimal degree formats. The mapping display shall have the ability to allow end users to create temporary features and annotation on the map, such as marathon routes, street closures, special events zones, with the ability for these to have predetermined expiration times. The mapping systems shall comply with NENA 71-501 v1, NENA 02-010 v9, NENA 02-014 v1.

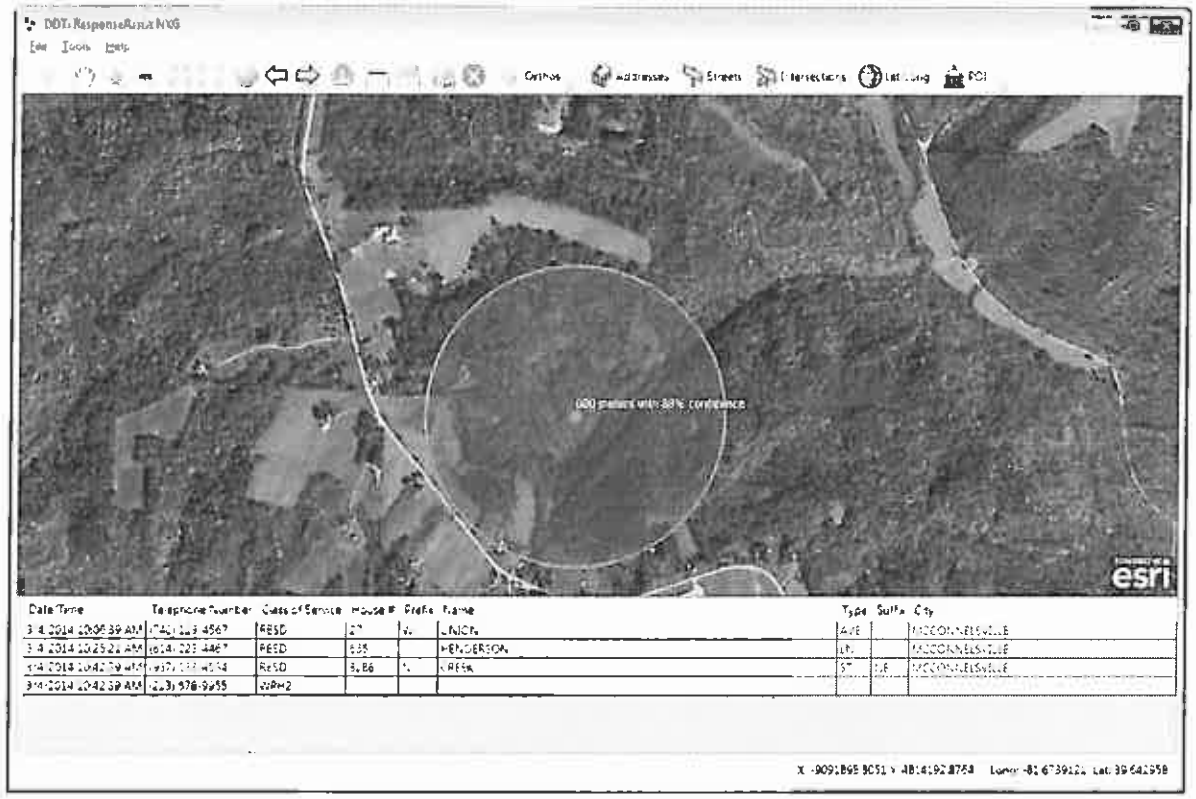
GDIT's proposed solution fully complies with the RFR requirements. GDIT's proposed solution includes the ESRI-based Tactical Map Display, called DDTi ResponseAssist NXG. The ResponseAssist NXG is based on the ESRI WPF 10.2 Runtime, and complies with all relevant NENA standards, including NENA 71-501 v1. The following screenshot shows the main map display window.

DDTi ResponseAssist NXG can utilize either ArcGIS 10.2 web services or locally deployed map packages created from ArcGIS. The software will consume ArcGIS web services from data published from the SIF. At a minimum, the SIF will provide the same road centerline and address GIS data used by the ECRF/LVF system and, thus, the map display has the same minimum data requirements as the ECRF/LVF. DDTi will also work directly with MassGIS to see what other data can be added to the system to increase the amount of information available to call takers (for example, railroads, hydrology, and fire hydrants).

The SIF will constantly monitor for changes in map data. When changes are detected, quality control operations run, and if the data passes quality control the data will be published to configured end points. These end points include the ECRF/LVF system, but they also include a Microsoft SQL Server instance that is used by ArcGIS Server. A dedicated virtual machine is used to create map tiles that are used by DDTi ResponseAssist NXG. The Microsoft SQL Server instance also provides the database used by ArcGIS Server for locator and feature web services,

which are also utilized by DDTi ResponseAssist NXG. Microsoft SQL Server replication technology is used for publishing data.

All payloads to the map will be in PIDF-LO format. ESRI locator services, either local or server based, are used for plotting call location in the case of a civic address PIDF-LO. Locator services can also be configured to allow users to search the map based on a street intersection. DDTi ResponseAssist NXG receives location data in the form of a PIDF-LO (although ALI is also supported) from the CPE server, parses the information, and calls one or more ESRI locator services to plot the call location. In the case of a geodetic location, a call to the server is not required, and the caller's location is plotted directly on the map. As PIDF-LO can contain more than one location, the user can toggle between the locations using the UI in the event that more than one location exists for a call. In the event of a legacy wireless call, the LDB (which communicates with a Mobile Positioning Center) will still deliver the Phase I and Phase II locations as PIDF-LO. The map can be configured to either overwrite the previous location or create a "breadcrumb" trail when performing a location rebid. All location data, regardless of the call payload type, will be in the form of PIDF-LO and can be consumed and plotted by DDTi ResponseAssist NXG. The following screenshot shows a legacy Phase II wireless call with confidence buffer display.



Standard ArcGIS tools are used to configure the web services consumed by DDTi ResponseAssist NXG and, thus, ArcMap connecting to the ArcGIS Server serves as the centralized administration point. Administrators within the PSAP can configure DDTi

ResponseAssist NXG for a customizable experience, by deciding which of the centralized mapping services they wish to use.

An interface is provided in DDTi ResponseAssist NXG to display data from an Integrated Pictometry Analytics (IPA) system (this service is provided by Pictometry and is not part of our proposed solution). When a call is plotted within DDTi ResponseAssist NXG, the window displaying the Pictometry imagery is automatically centered to the same location. The following screenshot shows the Pictometry IPA window.

The map can be configured to use external data sources providing they are supported by the ESRI components. Note that Google Maps is not free when used in an environment like this (only free for personal use).

As an option, the Commonwealth may utilize the ArcGIS Server web services that form part of this system to create their own custom applications. Additional licensing from ESRI may be required, depending on the ESRI Application Programming Interface (API) used.

At time of writing, the current version of DDTi ResponseAssist NXG is built on top of the ESRI 10.2 platform. As with other DDTi components, upgrades to DDTi ResponseAssist NXG will undergo testing in the GDIT i3 Solutions Interoperability Lab prior to any deployment to the live system. This often means there is a delay between ESRI delivering a new software version and deployment to a live system. DDTi will typically provide an upgraded version of the DDTi ResponseAssist NXG client to the GDIT lab for testing within three months of an official ESRI release.

DDTi ResponseAssist NXG allows users to search by address, intersection, common places (if the map data supports it) and latitude/longitude coordinates. Users can also hover over the map display to get latitude/longitude of a location (presented in various formats), as well as click on features to obtain more information about them (note, if the map is setup purely as tiles, this function is unavailable; feature services need to be used).

Basic drawing tools are provided to allow users to draw points, lines, polygons, and text on the map and to share the information with other users. Graphics can be set to expire and will automatically be removed from the map.

Discrepancy reporting as defined in NENA 02-014 is supported, allowing the user to generate a discrepancy report which includes a screenshot of the map as well as the raw location data (PIDF-LO). A free form text field allows the user to enter notes about the discrepancy. Reports can be routed to MassGIS over email.

DDTi ResponseAssist NXG has the capability to receive call location in legacy ALI formats as defined in NENA 02-010. However, it is expected that this new system will exclusively use PIDF-LO for location data.

8.7.24. Private Switch Automatic Location Information PS/ALI

The contractor shall, at a minimum, provide the same PS/ALI capabilities that are provided today to existing and new MLTS operators within the Commonwealth. The contractor shall provide a detailed transition plan from the legacy system and for existing customer base. The PS/ALI function shall allow for existing systems to connect without changes to their system.

The transition plan consists of two phases. The first phase requires the ESInet Location Database (LDB) to be populated with the Multi-Line Telephone System (MLTS) PS/ALI data. Each telephone number that may be transmitted as ANI or Calling Line ID (CLID) on a 9-1-1 call from a MLTS must be uploaded into the LDB database. This can be accomplished using the standard Service Order Processing function of the LDB (as detailed in Section 8.7.13, ALI Database Services), or by directly granting access to the LDB web interface to the operator of the MLTS. Using the web interface, the operator of the MLTS will be able to update location records for the numbers they have been assigned. All records must LVF validate, otherwise a discrepancy will be created and the location record or the GIS data must be fixed.

The steps of the first phase of the transition are:

1. Each MLTS operator will be configured as an entity with the LDB system by a system administrator.

2. One or more user accounts will be created for the MLTS operator, allowing them access to the LDB web interface and the ability to manipulate records associated with their entity.

3. If the MLTS operator has a small number of ALI records, the operator will be required to login to the LDB web interface and manually enter them. If the MLTS operator has a large number of ALI records, the operator will provide them to DDTi in either a NENA-compliant SOI format or an Excel spreadsheet. If using an Excel spreadsheet, it must contain the same data that is required by the NENA SOI format. DDTi will load the data into the LDB.

4. A user for the MLTS operator will login to the LDB web interface and verify all of their records are present and correct. The user will also verify that all records have passed LVF validation. Records that have failed validation will need to be investigated and corrected.

The second phase should not start until all records in the LDB are valid. The second phase of the transition requires the changing how the MLTS operators 9-1-1 calls reach the ESInet.

8.7.25. Interface to CAD

The response shall describe the interface to CAD. The CAD output shall conform to the State 911 Department's standard for ASCII output and shall be in format equivalent to legacy ALI data spills. Bidders shall quote CAD interface ports as both serial and Ethernet connections.

The CallStation system includes a modular, templated, event-based system for outputting data to third-party systems, including the support for ASCII output. The data link layer of these interfaces may be either serial (i.e., RS-232) or Ethernet. Emergency CallWorks supports a wide variety of Computer Aided Dispatch and Logging Recorder interfaces deployed in the field. The number of interfaces is expandable via IP and there is no practical limit to the total number of supported CAD outputs.

Please see pricing tables for CAD interface ports, both serial and Ethernet

8.7.26. Administrative Lines

The system shall support the following for each PSAP using the existing telephone numbers: The system shall support administrative lines using the local interface.

1. 2-Way Emergency Line: A ten (10) digit published emergency telephone number that displays ANI and ALI if the caller's line is not blocked. This line is the only outgoing line on the 911 system that allows for outbound calls; and

2. 1-Way InterPSAP Line: A non-published one-way line that is designated for incoming calls only. The line is used for PSAP to PSAP emergency communication.

See Attachment K2– Primary PSAP, Regional PSAP, and RECC Data for a list of the administrative lines in use at the time of issuance of this RFR.

The response shall describe in detail the proposed administrative line interface.

Any and all soft switches supplied by the contractor shall comply with the State 911 Department's regulations governing MLTS operators.

GDIT has included the support for administrative lines in our solution to support inbound and outbound (two-way) and PSAP-to-PSAP (one-way) calling form each call taker position. GDIT's solution also allows for local recording (using existing recorders) or (optionally) centralized logging and recording of administrative lines.

GDIT's solution provides for two administrative line methodologies. First, the CallStation CPE is a centralized IP PBX that will direct incoming NG9-1-1 traffic to each call taker position. The CPE will be provided with outbound PSTN SIP trunks to allow outbound calling from the CPE, with full integration of these administrative lines into the workstation, including the phone, headset, and activity screen. For example, call takers will be able to initiate callbacks to abandoned calls with a point-and-click from the activity screen. All outbound calling activity will be recorded and logged as is NG9-1-1 traffic.

GDIT's proposed solution also includes the deployment of a Cisco Unified Communications Manager (CUCM) in each data center, and equip each ESInet edge router with a survivable remote capability using local analog trunk interfaces. In this design, the central CUCM will provide all call control and processing in typical call flow, and all traffic will enter and leave the PSAP over the local PSTN connection, using existing phone numbers. The loss of the ESInet WAN will not have an impact on service locally, as the survivable gateway will provide call control and processing should the CUCM not be available.

The two methods are illustrated in Figure 53.

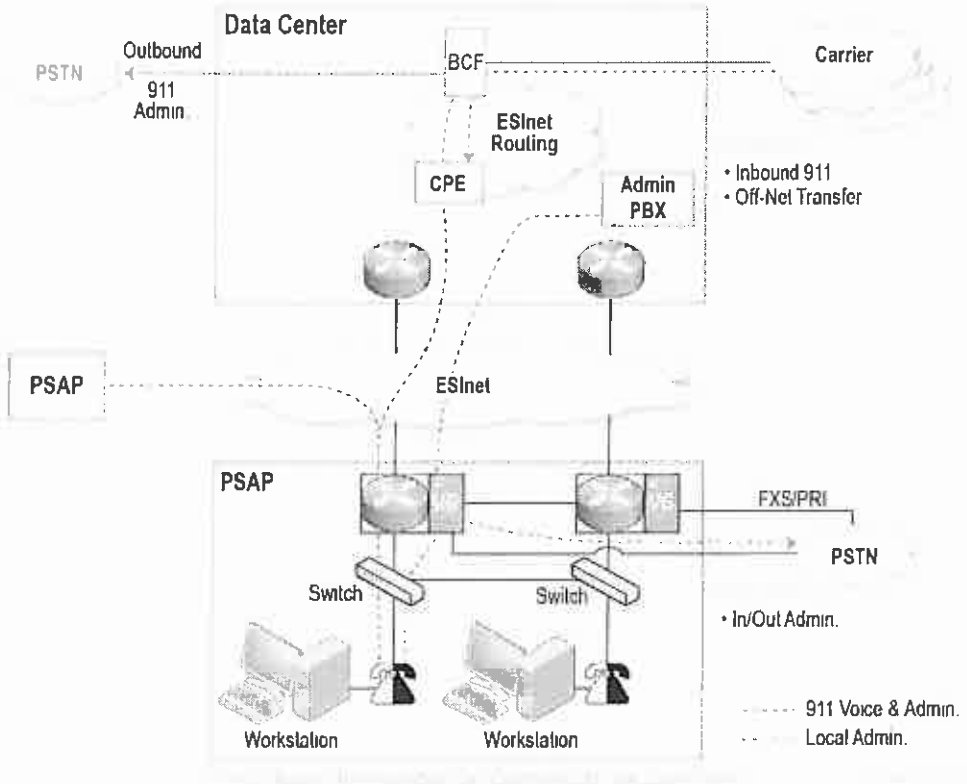


Figure 53. Administrative Line Support

8.7.27. Abandoned and Silent Calls

The system shall provide the following functions:

1. Abandoned Call Indicator that provides a visual and audio alarm that alerts that an Abandoned Call has been received;

2. Detection of DTMF Tones that displays corresponding digits on the screen (Silent Call Procedure); and

3. The ability to identify and answer TDD/TT/TTY and abandoned and silent calls including complete and accurate ANI and ALI of the TDD/TT/TTY calls.

The CallStation CPE provides sophisticated handling of abandoned calls. Calls which disconnect before answered are tagged with an "Abandoned" status, appear blue in the line organizer, and are sorted to the top of the list of calls available for answer. If mapping is used, the ANI with an icon will also appear on the map until cleared or recalled. Recalling is accomplished via a simple click on the call list or map icon.

If the call is from an uninitialized cell phone which does not provide a valid call back number, the abandoned call will automatically be cleared from the abandoned call queue. The system is also able to automatically determine if the call should be dialed back as a local or long distance call; this is especially important with more than 80% of all calls being wireless.

The Emergency CallWorks system manages TDD detection and processing via the VoIP back-end engine. This requires no specific TDD hardware or software at the call taker position. TDD detection is automatically performed on all calls handled by the system including E9-1-1, administrative, outbound, etc. TDD calls do not have any restrictions beyond regular calls, and TDD calls may be conferenced, making it possible for multiple call takers to participate in the TDD session. CallStation allows the conference and/or transfer of a TDD/TTY or TEXT call from one workstation to another, including transfers to another PSAP via the provided network. The caller's ANI/ALI information and any captured notes are also provided with the transfer.

Emergency CallWorks complies with Hearing Carry Over (HCO) and Voice Carry Over (VCO) for TDD calls. HCO and VCO are included at all times throughout the call and the call taker is not required to configure any settings for them.

CallStation includes a single button for initiating a TDD challenge. The standard challenge message is customer configurable, allowing the call taker to comply with a Silent Call SOP with a single button click. Full-time DTMF detection, logging, and display are also provided. All DTMF tones sent or received are time and user stamped and logged to the Call Detail. These logs are displayed in real-time in the Call Activity window and may be retrieved indefinitely as part of the Call Detail Report.

8.7.28. Audio Monitoring

The contractor shall provide an analog and digital demarcation point for third party audio applications and appliances to retrieve audio feeds from all trunks and administrative lines at PSAPs designated by the State 911 Department in its sole discretion. The demarcation point shall protect PSAP CPE and applications and appliances from any negative effects of such audio equipment. The PSAPs will be responsible for supplying audio equipment beyond the demarcation point. PSAPs that have been designated by the State 911 Department as requiring audio monitoring points are set forth in Attachment See Attachment K2– Primary PSAP, Regional PSAP, and RECC Data.

GDIT will comply with the Commonwealth's Audio Monitoring requirement.

8.7.29. Remote Ringer

The contractor shall supply, where needed, remote ringers at PSAPs to extend the audible ringing capability of the CPE to rooms outside of the communications area.

GDIT has provided a remote ringer as part of our optional priced solution.

8.7.30. Simultaneous Calls

The number of simultaneous calls delivered to the PSAPs shall correspond to the number of trunks set forth on Attachment K2 – Primary PSAP, Regional PSAP, and RECC Data, unless otherwise directed by the State 911 Department.

The number of simultaneous NG9-1-1 calls supported in GDIT's proposed solution is defined by the capacity limitations of each system within the ESInet. Starting with the PIF (gateways), GDIT's proposed solution provides TDM termination capacity at each data center to support 120% of all identified TDM trunks existing today in aggregate across all Commonwealth PSAPs. As discussed in greater detail in Section 8.7.1 (Routing Requests), GDIT assumes that the type of TDM terminations agreed to by the carriers will be 25% CAMA and 75% T1 or SS7. GDIT's proposed solution will seek to reduce the use of TDM trunks, and CAMA in particular, to avoid the expenditures on terminating systems (PIF) that will decrease over time and eventually be eliminated entirely from the end-state architecture.

Termination of incoming IP traffic from the carriers greatly reduces the limitation of capacity associated with the PIF, and brings the ESInet architecture closer to the NENA i3 end state. With IP interfaces, the PIF is bypassed and terminated directly on the BCF. The BCF will also take all call ingress traffic that comes from the PIF. The BCF pair at each data center supports 8,000 simultaneous calls.

ESInet components necessary in routing decisions, including the ESRP, ECRF/LVF, LDB, and LIF/NIF, provide and insert location information (by reference and by value), but do not typically receive call media. These components are sized to provide active routing and mapping in excess of 1,000 simultaneous calls in each data center

The CallStation CPE receives media from the BCF and routing and mapping information from the ESInet components. CallStation as proposed supports in excess of 1,000 active calls concurrently at each data center. Greater than 4,000 additional calls may be held in queue, allowing each call taker position to manage as many as five calls simultaneously.

As a result of these design considerations, each data center is equipped to deliver in excess of 120% (1,000) of total call taker positions existing in the Commonwealth (~830) and approximately 4,000 additional calls held in queue.

Administrative calling is sized to support 100 off-net simultaneous calls from each data center, using PSTN trunks provided to the data centers (via Windstream). Administrative station-to-station calling within and across PSAPs, and off-net through the data center trunks is licensed to support over 500 simultaneous calls from each data center using the ESInet WAN, and capable of expanding. Simultaneous off-net PSTN calls using local PSAP trunks are provided through the survivable gateway functions associated with the CUCM. The CUCM is configured to support 500 simultaneous calls per data center, although it is limited to the number of available trunks on a per-site basis. The number of trunks is identified in Table K2 of the RFR.

8.7.31. Limited Secondary PSAP Equipment

The system shall provide equipment that offers only the following limited functionality for limited secondary PSAPs:

1. *Read-only display of ANI/ALI;*
2. *Laser printer for printing of ANI/ALI displays; and*
3. *Global setting for automatic print option that can be managed by the PSAP and users.*

Data sent to a limited secondary PSAP cannot be re-routed to another location. The limited secondary PSAPs shall be connected to the ESInet.

Today, the "Limited Secondary" PSAPs are receiving voice transfers via standard analog administrative lines augmented with an ALI location feed over a separate leased data line into either a terminal emulator or serial printer. Due to the point-to-point nature of the existing leased lines, limited secondary PSAPs are only able to receive transfers with location from only one or two PSAPs. Furthermore, limited secondary PSAPs are not able to transfer calls back to primary or secondary PSAPs in the event of a mis-transferred call or a moving caller. Currently there is limited to no ability to track times or dispositions of calls after they are transferred out of the 9-1-1 system to a limited secondary PSAP.

GDIT's proposed solution provides an ESInet connection to each Limited Secondary PSAP, with an edge router, an IP phone with reader display, and a network printer. In this manner, any PSAP can transfer and/or conference a call to a Limited Secondary PSAP and initiate a print of ALI information and mapping as required. All activity to the Limited Secondary PSAP will be included in the logging and reporting centrally. Re-routing of traffic to the Limited Secondary PSAP will be disabled.

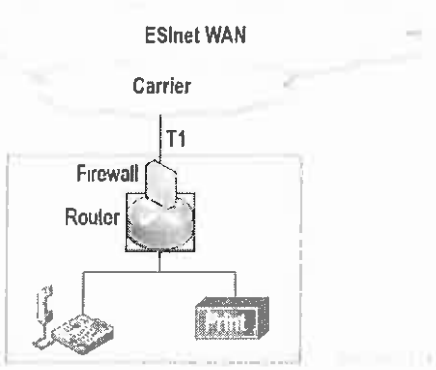


Figure 54. Limited Secondary PSAP

The CallStation system provides sophisticated message routing and templating capabilities that allow for interfacing to any of the existing systems within the limited secondary PSAPs. With this, information can be provided to the Limited Secondary PSAP in any format desired.

Figure 55 shows the Polycom 650 display:

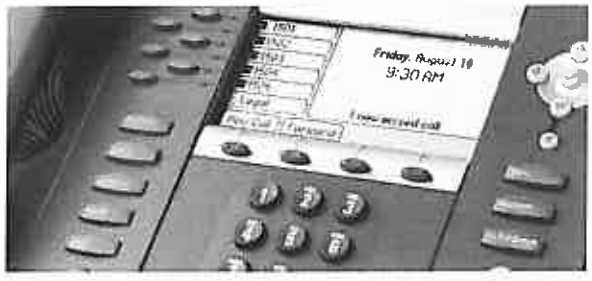


Figure 55. Polycom 650 Display

8.7.32. Mobile PSAP

The contractor shall equip, install, monitor, and maintain the mobile PSAP. The contractor shall be required to respond to and/or provide services at any location identified by the State 911 Department throughout the Commonwealth. Mechanical repairs and service of the vehicle are procured through a separate procurement mechanism.

GDIT will equip, install, monitor, and maintain the mobile PSAP. To accommodate the specific requirements of the mobile PSAP for operating in deployed and post-deployment (simulation) modes, GDIT's design will enable the mobile PSAP to seamlessly function and transition between the two environments. Similar to the traditionally stationary PSAP, the mobile PSAP will be equipped as a complete NG9-1-1 Call Taking Platform, capable of receiving and servicing calls from both legacy E9-1-1 as well as i3 NG9-1-1 interfaces. In addition, the equipment and software configuration will be such that the mobile PSAP will have no outside dependencies and will be fully functional in deployment or post-deployment (simulation) mode with or without network access.

GDIT's proposed solution for the mobile PSAP will provide access to the ESInet (ESRP, LDB, etc.) including a VPN tunnel established over the Internet via the three (3) types of network connection, with an optional third:

1. Primary – direct wired
2. Secondary – Wi-Fi
3. Tertiary – 3G/4G.
4. Tertiary (optional) – Satellite

GDIT's solution uses wired, Wi-Fi, and 3G/4G to provide cost savings, reliability, and operational simplicity. The 4G Long-Term Evolution (LTE) wireless upgrade will be provided as part of our solution for the mobile PSAP. The (optional) satellite configuration will provide a 2 MB connection to the data center, and it requires each data center to have satellite access. The optional proposal includes the mobile PSAP antenna. The data center antennas are 'shared use' and must be identified separately. Further, the PSAP antenna provides GPS auto aiming that will eliminate the need for manual antenna adjustment, and which will only operate while the PSAP is stationary. An illustration of the Mobile PSAP configuration is shown in Figure 56.

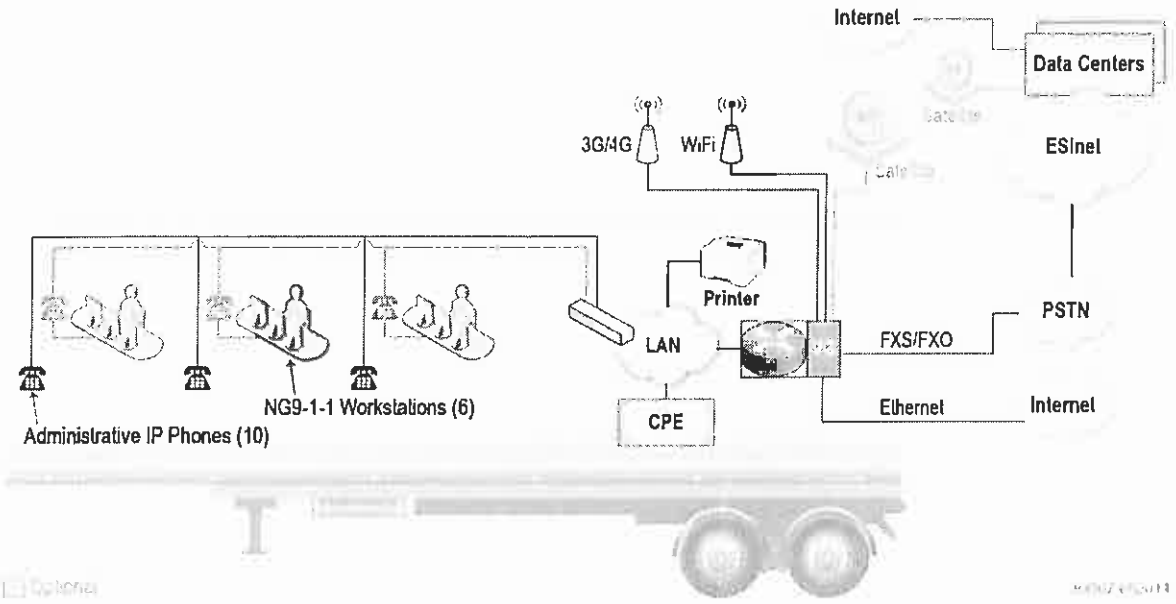


Figure 56. Mobile PSAP

Section 8.7.32.2 (Installation Requirements) provides details about the equipment and ancillary components to be installed in the mobile PSAP as part of the proposed solution.

8.7.32.1. Administrative Telephones

The mobile PSAP equipment shall include ten (10) administrative IP phone sets, acting independently from the 9-1-1 function. The administrative phones will be used for the purpose of terminating analog POTS lines. The mobile PSAP has CAT5 cabling and multiple RJ45 ports located throughout the vehicle.

GDIT will comply with the RFR specification to provide ten (10) administrative phone sets that will operate independently from the 9-1-1 functionality of the other sets in the mobile PSAP. These administrative VoIP phones will terminate to analog POTS lines through the Cisco 2901 router installed as part of the mobile PSAP suite of equipment as described in Section 8.7.32.2. The Cisco router will include a survivable gateway bundle that includes analog termination cards for TDM connections to the PSTN and the voice services bundle for connection to the data center's CUCM. This will allow for termination of analog trunks to the PSTN for administrative inbound/outbound voice without a connection to the ESInet. The administrative VoIP phones will connect to the Cisco router via the use of a locally mounted patch panel, CAT5 cabling, and the multiple RJ45 ports located throughout the mobile PSAP. The Polycom 650, a SIP desktop phone set, is proposed for administrative lines; it will provide six line appearances (expandable to 12) and a color display. Each phone set will offer features similar to a common business set including but not limited to inward and outward dialing, conference, hold, mute, caller ID, and speakerphone. Figure 57 provides a picture of the Polycom model 650 SIP telephone instrument.

Figure 57. Polycom 650 SIP Telephone

GDIT offers the optional configuration of 'dual registration' for the Polycom 650. In this configuration, a single shared use Polycom 650 would be used as both an administrative and NG9-1-1 phone by defining a number of line appearances as NG9-1-1 and the rest as administrative. This configuration would reduce space and complexity for the call taker positions, and it can be provided on some or all of the phones.

8.7.32.2. Installation Requirements

For the installation of mobile PSAP CPE, the testing process, acceptance process, and the schedule for installation of mobile PSAP CPE shall be established by the State 911 Department.

GDIT understands the RFR requirement and will fully comply. We will develop the testing and acceptance process and validate with the State 911 Department to ensure compliance with State 911 Department approval processes. We will also comply with the schedule as outlined by the State 911 Department for installation, testing, and acceptance of the mobile PSAP CPE. Table 7 provides the hardware additions that GDIT will equip, install, test, monitor, and maintain as part of the mobile PSAP solution.

Table 7. Equipment List: Mobile PSAP

Part Number	Description	Quantity
NG911GL84OES-KIT	Equipment Cabinet Kit (GL840ES-2442MSS)	1
C2901-VSEC/K9	Cisco 2901 Router	1
VIC2-2FXO	2-port FXO voice/fax interface card	1
VIC2-4FXO	4-port FXO voice/fax interface card	2
PVDM3-16	16-Channel high-density voice and video DSP module	1
EHWIC-4G-LTE-G	4G LTE EHWIC for Global, 800/900/1800/2100/2600 MHz	1
4G-AE010-R	Single Unit antenna Extension Base (10 foot cable included)	2
4G-LTE-ANTM-D	4G LTE articulating dipole antenna 700MHz-2600MHz bands	2
WS-3650	Cisco 3650 Ethernet Switch	2
B020-008-17	Rack Console with KVM switch	1
R620	Dell R620 Server	2
DCB	Analog Gtwy (IAD)	1
Lantronix	CAD Interface Module	1
MCMK00015-Single	Rack Shelf, Misc	3

Part Number	Description	Quantity
EXC100001-NS	Audio Interface Unit (AIU)	6
Dell 3020	OptiPlex 3020, Workstation	7
P2414H	Workstation Monitor	14
AC511	Sound Bar	7
2200-12651-025	Sound Point IP 650	17
CS 540-XD	Headsets	7
Laserjet Pro 400	Network Printer	1
4G-CAB-ULL-20	20-ft (6m) Ultra Low Loss LMR 400 Cable with TNC Connector	7
CGR-LA-NM-NF	Lightning Arrestor Kit: male to female	1

The Pre-Installation and Staging effort for the mobile PSAP will include:

- Installation and configuration all components for the mobile PSAP in the staging area
- Power on of equipment, verification of configuration, settings, and system burn-in for a minimum of seventy-two (72) hours
- Provide the results of the full system staging test to identify any component failures encountered and on what test attempt the system passed the test at least forty-eight (48) hours prior to the installation at the PSAP

The physical installation effort for the mobile PSAP will include:

- Installation of rack accessories to accommodate horizontal and vertical cable management
- Installation of all new PSAP system hardware/software
- Installation of all new call taker position hardware/software
- Installation of system cabling to include termination, dressing, and labeling
- Installation of WAN circuit demarcations for data center to PSAP connectivity
- Power-up of system components
- Perform final configuration of system components for optimization, updates, etc.
- Perform and complete pre-cutover dry run
- Provide a backup procedure to ensure that all data has been appropriately backed up after all configurations are final; completed at least forty-eight (48) hours prior to the scheduled cutover date
- Perform and complete acceptance testing

The configuration management and documentation effort for the mobile PSAP will include:

- Network parameters, such as IP address, VLAN, and subnet assignments
- Security/routing configurations
- System-specific configuration details
- WAN circuit connectivity
- Site-specific configuration details
- Network integration details for domain controller, NTP, DHCP, and Syslog (as applicable)

- Other parameters necessary to integrate each functional element into the overall NG9-1-1 architecture, such as uplink type and speed
- Bill of Materials (BOM)
- Project drawings (to include equipment floor plans, signal, and power cabling, etc.)

8.7.32.3. Deployment Configuration

At the request of the State 911 Department, the contractor shall reconfigure the mobile PSAP CPE and/or software for deployment.

GDIT understands the requirement for transitioning between post-deployment and deployment configurations. At the request of the State 911 Department, GDIT will provide all technical resources necessary to successfully complete the transition from a post-deployment configuration to an operational deployment configuration.

The mobile PSAP's proposed configuration will include a fully autonomous (dual cluster) server platform and redundant CPE implementation at all of the call taker position workstations. This design will allow for an increased level of survivability with the added benefit of being able to operate either completely stand-alone or interconnected through the new ESInet. During "Deployment" operations, the mobile PSAP will be connected via direct-wireline, Wi-Fi, or 3G/4G (situation/location dependent) to the ESInet and will be able to perform the same capabilities as any traditional PSAP.

8.7.32.4. Post-Deployment Configuration

At the request of the State 911 Department, the contractor shall reconfigure the mobile PSAP following deployment so that the mobile PSAP may be utilized for demonstration purposes.

GDIT's understands and will comply with the RFR specification. At the request of the State 911 Department following any deployment scenario, GDIT will provide all technical resources necessary to successfully complete the transition from a deployment configuration to a post-deployment configuration that will allow the mobile PSAP to be utilized for training and demonstration purposes. Section 8.7.32.5 (Simulated Environment) provides details about the simulation software to installed and configured as part of the proposed mobile PSAP solution.

8.7.32.5. Simulated Environment

The contractor shall provide a simulated environment for simulated call answering. The simulators shall simulate the transmission and answering of 911 payloads, and shall provide ALI and mapping.

For post-deployment operations, GDIT understands the requirement for a call simulation environment to create live environment situations for demonstrations and training for 9-1-1 operators. The mobile PSAP's post-deployment configuration will include Emergency CallWorks IP-based, designed, and integrated call simulation software, which will he hosted on the dual-cluster server platform. While operating in a simulated environment, a separate call handling group will be established and configured such that calls will be directed towards the Emergency CallWorks simulator. The software will simulate both the transmission and answering of 9-1-1 calls providing ANI, ALI, and mapping. A separate inbound text capability is also provided to test and train inbound text messaging workflow and training. Once configured, the simulation software can be utilized at any time, on-demand as needed.

8.7.32.6. Terminating Analog Lines

In addition to operating in an all-IP scenario, the mobile PSAP CPE shall have the ability to terminate analog telephone lines. Bidders shall describe in detail how they shall meet these requirements.

Each primary and secondary PSAP, including the Mobile PSAP, will utilize a Cisco router to connect to the ESInet and provide monitoring points for network and security management. Specifically for the Mobile PSAP, GDIT's proposed solution includes ESInet connectivity using Ethernet, WiFi, and/or 3G/4G through interface modules/functionality of the Cisco router.

The Cisco 2901 will also be include one (1) VIC2-2FXO 2-port and two (2) VIC2-2FXO 4-port interface cards that will allow for the termination of up to ten (10) analog POTS lines to support administrative calling inbound and outbound. This 'voice gateway' capability will be managed as stand-alone gateways when there is no ESInet connection, and it will be managed by the data center CUCM when the ESInet is connected. The administrative Polycom 650 VoIP phones are included as part of the Mobile PSAP suite of equipment, and they will connect to the Cisco router via the use of a locally mounted patch panel, CAT5 cabling, and the multiple RJ45 ports located throughout the Mobile PSAP. This end-to-end configuration will provide dial tone to/from the analog POTS lines, through the Cisco 2901 router UC/PBX, and to the to the VoIP phone sets.

8.7.32.7. UPS Maintenance

The contractor shall replace the mobile PSAP batteries upon the manufacturer's recommended interval and immediately upon malfunction or failure. The contractor shall perform a preventative maintenance including recommend firmware updates. UPS shall be monitored using SNMP traps via the existing Ethernet network interface card installed in the UPS.

GDIT understands the requirement and will replace the mobile PSAP's newly installed UPS batteries upon the manufacturer's recommended interval and immediately upon malfunction or failure. Table 8 provides the new UPS equipment that GDIT will equip, install, test, monitor, and maintain as part of the mobile PSAP solution.

Table 8. Equipment List: Mobile PSAP – UPS

Part Number	Description	Quantity	Maintenance/Replacement Interval
SMX1500RM2U	UPS, APC 1500VA, (Call Taker positions)	7	Maintenance-free; sealed lead-acid battery with suspended electrolyte; leak proof. Replacement battery: APCRBC115; Expected battery life: 3–5 years
SMX3000RMLV2U	UPS - Smart-UPS X 3000VA	1	Maintenance-free; sealed lead-acid battery with suspended electrolyte; leak proof. Replacement battery: APCRBC117; Expected battery life: 3–5 years
SMX120RMBP2U	UPS Extended Battery	1	Maintenance-free; sealed lead-acid battery with suspended electrolyte; leak proof. Replacement battery: RBC17; Expected battery life: 3–5 years
SBP3000RM	APC Service Bypass PDU	1	N/A

8.7.32.8. Spare Parts

The contractor shall manage a spare parts inventory for the mobile PSAP. The spare parts shall be located on the mobile PSAP or at a mutually agreed upon location within Massachusetts.

The inventory process shall be mutually agreed to by the parties.

GDIT will maintain an adequate inventory of spare parts to ensure expedient repair of the system and guarantee that any replacement or upgrade of spare parts will be available for the term of the

contract. Should a manufacturer discontinue any product or cease to do business, GDIT agrees to stock an adequate supply of replacement components. To account for the mobile PSAP's mission and ability to travel to various locations around the state, GDIT understands that immediate access would be of the utmost priority to ensure the availability of critical system components in the event of a failure. For this reason, the provided spare parts will be stored locally in the mobile PSAP. Table 9 identifies the spares that GDIT will provide as part of the mobile PSAP solution.

Table 9. Equipment List: Mobile PSAP – Spares

Part Number	Description	Quantity
341-9253	Hard Drive - Dell R620 Server, Serial ATA, 500MB, 7200 RPM	1
331-5929	Spare Power Supply - Dell R620 Server	1
2200-12651-025	POLYCOM 650 SIP PHONE	1
CS 540-XD	Headset, Wireless, Over the Ear	1
EHWIC-4G-LTE-V	4G LTE EHWIC for Verizon, 700 MHz Band 13 / CDMA	1

8.7.32.9. Mobile PSAP CPE Monitoring

The contractor shall provide mobile PSAP CPE monitoring upon the request of the State 911 Department at the time of deployment of the mobile PSAP. The State 911 Department will notify the contractor of the deployment of the mobile PSAP. All monitoring shall be provided through a secure IP connection provided by the contractor. The State 911 Department will provide an Internet connection. The contractor shall ensure that alarms will be received and monitored through a central monitoring location.

In addition to the monitoring services during deployment of the mobile PSAP, the contractor shall provide standby mobile PSAP monitoring when the mobile PSAP is inactive. The contractor shall perform remote maintenance to further investigate alarms and/or reset alarms. The contractor shall proactively monitor and manage the mobile PSAP CPE for impending failures to mitigate minor alarms from becoming major alarms. The contractor shall work cooperatively with the State 911 Department to properly classify and respond to alerts and alarms.

GDIT will integrate the Mobile PSAP into the overall proposed network and security monitoring solution. While IP connectivity will be required to perform this function actively, information can also be stored during offline usage and investigated upon future connection. GDIT proposes the SolarWinds monitoring suite for network performance and AlienVault for security monitoring surveillance level systems. Monitoring will allow for monitoring, diagnosing, troubleshooting, and repairing many of the errors both known or unknown to the mobile PSAP. CallStation also includes an integrated "Reverse VPN" solution that automatically establishes a secure and encrypted connection to its configured management and monitoring server any time an Internet connection is available. When the system in not in active use, the monitoring server has the capability to designate the system as "out of service," such that faults and performance are still monitored, but real-time notifications are not dispatched to technicians. Through the use of this monitoring system, on-site service repairs and/or replacements will be provided when and where they are identified.

8.7.32.10. Additional Mobile PSAP Services

At the request of the State 911 Department, the contractor may be required to provide additional services to support the mobile PSAP. The contractor shall complete the requested services through a separate statement of work to be negotiated by the parties at the time of request.

GDIT will provide all technical resources necessary to provide additional services to support the mobile PSAP via a separate statement of work to be negotiated by all parties at the time of request.

8.7.33. Administrative Positions

The contractor shall provide and maintain an administrative position at each PSAP. The administrative position shall be used to access reporting functions and other administrative or maintenance functions. The administrative position shall be equipped with a CDRW drive.

The GDIT team will plan for and create an administrative position at each of the PSAPs. The credentials for this administrator user will include permissions to run and print reports, perform maintenance functions, and store or access data from a locally equipped Compact Disc, Rewriteable (CDRW) drive.

8.7.34. User Logins

The State 911 Department shall have the ability to add or remove user logins, and reset passwords for all PSAP positions from a remote location. PSAPs shall not have access to modify user logins. Bidders shall identify in the response the mechanism and processes for managing user logins for PSAPs.

The GDIT team proposes the AdminiStation web-based tool as the solution allowing any authorized user to log in from any location of which the network is accessible and configure a wide variety of parameters, including all user settings such as user ID, password, and roles/permissions.

The AdminiStation solution provides centralized storage of all configuration data. However, particular data and settings that are relevant only to a specific "dispatch group" (typically a single PSAP) will only be able to be seen or modified by users in that dispatch group or administrators who have authority over that dispatch group. All control is done by login; the location from which the data is accessed is not relevant to the system. All configuration changes may be affected from anywhere within the network. Permissions will be set to disallow PSAP personnel from modifying user logins. All modification requests will be made through the GDIT 24x7 NSOC and implemented upon an established approval process.

8.7.35. Auto Dial Entries

Each PSAP shall have the capability of administrating its own auto dial entries. Access to administrative configuration tools for PSAPs shall be limited to adding, deleting or modifying the auto dial entries at their respective location. The contractor shall identify any limits placed upon the number of entries available.

The GDIT team supports administration of auto dial entries via the AdminiStation web-based administration tool. Up to six single-click intelligent transfer buttons can be configured on the main call control screen. Within the easily accessible directory, up to eight large buttons can be configured for each of the unlimited categories. Each category may also contain an unlimited number of entries (eight of which are associated with the aforementioned buttons).

8.7.36. Headsets/Handsets

At the request of the State 911 Department or an eligible entity, the contractor shall provide headsets/handsets, both wired and wireless, for use with the CPE. Bidders shall provide optional pricing for such headsets/handsets. The contractor shall provide an interface to public safety radio systems.

The GDIT team provides a SoundPoint 650 VoIP phone as a backup to the Intelligent Workstation. A Plantronics CS540-XD wireless and a Plantronics C720 wired headset is provided optionally to support the phone. GDIT's solution includes an Audio Interface Unit (AIU), which allows users to use only one headset/handset while interfacing with the Commonwealth-provided public safety radio systems.

8.8. SYSTEM ADMINISTRATION

The response shall describe the overall system administration. The response shall address each of the subcategories below. System administration is intended to include all aspects of system monitoring and pro-active fault prevention. This service shall be provided 24 x 7, and shall act as the single point of notification for all system issues.

GDIT's system administration capabilities provide comprehensive and fully compliant system monitoring and proactive diagnostics and reporting capabilities that will be customized based the State 911 Department's operational requirements.

GDIT has been providing mission-critical network operations to the DoD, federal agencies, and state and local governments from our Fairview Heights, IL NOC for over 20 years. We have established unparalleled expertise and capabilities in delivering support to our clients that range from full remote and on-site operational responsibility to advanced Tier III support to a Tier I 24x7 call center. The GDIT NOC retains highly trained staff (who hold OEM and industry certifications, are U.S. citizens, and hold DoD security clearances) in a wide array of OEM products, technologies, and operational constructs, including proactive network monitoring and security management. Further, we retain direct relationships with all OEMs and with support and technical staff, which enables us to gain support, visibility, and awareness that few others can achieve.

Security management is critically linked to network management, with the expected difference being the purposes of analyzing information and a (very) few differences in the tools and mechanisms used to collect and present information to administrators. As such, much of this discussion merges both network and security management constructs, which are highly interrelated and each critical in their own right to defining the overall NG9-1-1 architecture, configuration, setup, and use.

Robust centralized operations and security management are fundamental enablers of GDIT's proposed NG9-1-1 solution, reducing maintenance costs, improving service responsiveness, providing critical operational visibility, and ensuring reliability. Where the traditional E9-1-1 construct leverages redundant instances of independent systems, local carrier connections, and local staff, the effects of convergence and centralization delivered within the NG9-1-1 ESInet architecture offer a dramatically improved operations model. The consolidation of systems and intelligence to the service delivery point (e.g., data centers) reduces maintenance points, aggregates and reduces carrier trunks, and increases operational control across the network.

The GDIT Network and Security Operations Center (NSOC) solution defines a holistic systems integration approach supporting both the network and security management considerations that include systems configuration, traffic conditioning, administrative control mechanisms, and data collection. Our approach leverages the best practices developed for managing high-reliability, low-cost, and distributed networks as defined with the Telecommunication Management Network (TMN) architecture defined by Telecommunications Standardization Sector (ITU-T) for managing open systems in a communications network. Within this construct, the Fault, Configuration, Accounting, Performance, Security (FCAPS) model defines the functions and capabilities necessary for comprehensive operations management. FCAPS identifies the following capabilities as necessary for comprehensive network management:

- Fault Management
- Configuration

- Accounting
- Performance
- Security

Fault Management

Fault management includes mechanisms for monitoring the health of the network and services and for providing targeted reactive maintenance to a range of conditions. Information and notification of network conditions are received from one of two sources: OEM systems and traffic monitoring. Faults and conditions are reported by individual systems through management messaging and generated logs. This self-reported information is collected, analyzed, and reported by the identified Operations Support System (OSS) tool set.

The benefits of centralized operations in the NG9-1-1 architecture extend beyond building efficiencies and controls to becoming an integral component of the service reliability model. Traditional E9-1-1 (TDM) services are "deterministic," where service is (largely) either working or not, subject to "hard" failures that are highly apparent and allow for reactive maintenance. Rarely in the traditional environment will services be working but of marginal quality.

Unlike TDM, the IP services model has the additional burden of involving a wide range of "soft" conditions that are both transient in nature and granular in severity. In large part, these conditions are the result of contention for shared resources across the entire IP services domain. Various techniques, including network engineering, traffic management, and access control, provide an excellent approximation to a deterministic environment. However, the only means for validating service quality, particularly for real-time services of voice and video, is through real-time monitoring of every session. Such monitoring can determine hard failures for reactive maintenance, but equally important, it can provide critical trending analysis of Key Performance Indicators (KPIs) that allows proactive maintenance to prevent future problems. Monitoring for proactive maintenance is, therefore, a key component of the service assurance model. It should be noted that monitoring is also a critical mechanism for security management and for managing Service Level Agreements (SLAs) at network boundaries.

Configuration

Configuration of systems and provisioning of services to support changes to the environment – including Moves, Adds, and Changes (MACs) and system settings – are critical components of the network management environment. GDIT's proposed centralized operations and management solution leverages the combination of OSS tools, vendor-specific Element Management Systems (EMSs), and IP networking techniques (Network Address Translation (NAT), subnetting, Virtual Local Area Networks (VLANs), etc.), and the creation of standardized configuration practices to centralize and simplify these efforts. Such change management is supported by centralized administration to ensure and track privileges, and logging to remediate any erroneous or malicious activity.

Accounting

Accounting is concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes. While this is not appropriate in the NG9-1-1 environment, gaining knowledge of call taker activities, both real-time and historical, is fundamental to operational efficiencies and

possibly a legal necessity. Therefore, administration and authorization are used to define a set of capabilities for tracking usage statistics and ensuring strong, trackable privileged use and participation in the NG9-1-1 environment, to include user accounts and passwords, and permission management. GDIT has included a centralized Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) model.

Performance

Understanding the health and capacity of the network to support active services, or the unknown demand for future services is fundamental to network performance. Real-time services such as voice and video are sensitive to transmission delay, something that can be caused by bursts in data traffic (a burden associated with converging multiple service types onto a single physical and logical infrastructure). Managing network performance requires understanding the quality of services, capacity of the network, and ability of the network to react to new service demands. In order to deliver these capabilities, information must be available from every element pertaining to past and active services, and an expectation for future services can be achieved. GDIT's management solution leverages the same set of self-reporting mechanisms required for fault management, standards-based SNMPv3 where available, and other management messaging to collect the network information, in addition to traffic inspection performed at the ingress and egress of each location. This information is reported and collected by the OSS systems deployed at the NSOC to offer necessary management visibility and control. The systems include Splunk forwarding and indexing, and comprehensive set of SolarWinds management systems.

Security

GDIT's information security approach is built upon our extensive experience deploying and defending mission-critical information networks for federal and DoD customers. We are committed to a risk-based approach to mitigating threats to NG9-1-1 services and information guided by NENA 75-001 and 002, and leveraging best practices developed in other mission-critical environments.

Our defensible network approach (Section 8.4) provides visible and known points of entry (demarcation), thereby removing uncontrolled avenues of attack. Centralized policy-based traffic controls are pushed to all boundaries and systems to ensure a consistent and systemic approach. The components of the defensible network are configured and maintained in accordance with a standard baseline, as stated in NENA 75-001, for security of NG9-1-1 networks, to ensure that the prescribed security mechanisms, traffic configurations, and control points provide information assurance.

Where traffic management and control is critical to protecting the boundaries, a defense-in-depth approach must also consider internal threats and some level of threat penetration. As such, monitoring and vulnerability scanning become critical to identify, track, limit, and remediate threats. Such monitoring is highly similar in data flows and capabilities to network management monitoring, leveraging reporting from systems and inspection of packets to make determinations. Therefore, security-based tools operate in parallel to network management-based tools using highly coordinated tools and overall network design to ensure appropriate performance.

The following is a partial list of capabilities, mechanisms, and considerations that are key enablers of GDIT's proposed solution in achieving a proactive network and security management construct in compliance with NENA standards:

- **Border Control Function (BCF)**: BCF is a required component of the ESInet architecture and serves as a dynamic firewall allowing voice services paths to be created and closed upon demand. In addition to ingress and egress protection at the data centers, the GDIT solution also places a BCF at each PSAP to offer an incremental level of protection beyond NENA standards.

- **Edge Router/Firewalls**: These provide the demarcation at each site for data routing, enabling resilient and secure traffic management, including Quality of Service (QoS) management, stateful firewall, encryption, and traffic separation.

- **Central Policy Enforcement Point (PEP)**: GDIT's proposed solution recommends the flow of all Internet traffic to/from all ESInet connected systems to be forced through a centralized PEP, where traffic can be monitored, filtered, and secured. Centralizing the connection will also reduce cost for individual PSAP Internet connections. GDIT's solution proposes the use of the Cisco ASA firewall at the data center for all Internet traffic.

- **Intrusion Detection and Prevention (IDP)**: This is an advanced security function that allows traffic to be inspected at network boundaries for known viruses, policies, and malicious attack profiles. GDIT's solution provides IDP as an integrated component of all routers at every site even with Internet traffic forced to the data center routers, given the possibility (expectation) of connecting other private or public networks to the ESInet.

- **Logging**: Each system in the GDIT solution is configured to create and send logs on all system operations, including administrative access and changes, capacity reports, and systems health. These logs are collected, indexed, and stored as critical pieces of input for both security and network management.

- **Encryption**: Data encryption utilizing IPsec is provided on all IP services leaving the PSAP or data center in compliance with NENA standards, such that no information is decipherable should it be intercepted. Encryption is supported with anticipated use of L3 Virtual Private Network (VPN) tunnels to increase privacy and provide critical separation of traffic by types across the IP WAN.

- **Messaging**: SNMPv3 is defined by NENA as the protocol for management messaging. While not all components of GDIT's solution presently support SNMPv3, each component has a roadmap to offer this capability in the future. Until then, SNMPv1 or 2c, Web Management Interface (WMI), or other messaging protocols will be used. To support the privacy of these messages (intended by SNMPv3), traffic will be encrypted at the data layer.

- **Storage**: This is a critical component for network and security management and is a historical archive for event logging recording. Centralized storage offers a vastly superior ability to efficiently manage and use historical information, including backup, aging, and retrieval. GDIT's proposed solution places approximately 10 TB of mirrored storage at

each data center, and is expected to support over five years of operations without any aging of files.

- **Authentication and Authorization**: GDIT's proposed solution includes a policy-based Active Directory (AD) environment to provide centralized Authentication, Authorization, and Accounting (AAA) for managing access to the all systems for all privileged users, including administrators, supervisors, and call takers. GDIT's proposed solution employs a redundant, centralized, and role-based authentication policy engine to manage access of all users, from all locations, to all (capable) devices. The solution will leverage a Microsoft Active Directory (AD) group management policy, maintained at (redundant) master domain controllers at the data centers. The AD will authenticate users with their associated role-based mapping on both RADIUS and LDAP enabled systems. Systems not capable of LDAP or RADIUS will be maintained independent of the AD structure.

- **Vulnerability Management**: The network is subject to threats form external and internal penetration, or from erroneous internal behavior that typically results in changes in network configurations. Vulnerability scanning performs analysis of the network to identify unauthorized changes and/or security policy violations and activity that may indicate either a potential threat or an active threat. Vulnerability management is being performed by the AlienVault system, residing in each data center.

- **Security Incident and Event Management (SIEM)**: SIEM functionality performs analysis of management traffic flow, including SNMP, WMI, Syslog, netflow, IPMI, ICMP, and SSH and other systems reporting mechanisms to present a critical view of events and traffic flow that allows for both real-time and historical monitoring. GDIT will leverage the AlienVault systems to collect, index, and report on information provided by all systems through logging and messaging.

- **Network Services**: The need for IP network services is a critical enabler of services reliability and quality, which also has security and network management considerations. All network services to ensure industry best practices and NENA compliance are included in GDIT's proposed solution, including:

  — Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are provided in a redundant configuration from the domain controllers located within each data center.

  — IP Address Management (IPAM) is supported through the SolarWinds OSS platform.

  — Network Time Protocol (NTP) is provided through redundant, NENA-compliant master clocks located at each data center and primary/secondary PSAP.

- **Update and Download Server/Solution**: Most, if not all applications, devices, and services within the proposed environment require periodic and/or recurring updates. Some of these services, such as McAfee AntiVirus and Windows Server OS, have particularly regular and/or time-sensitive update requirements, necessitating automated updates. Update and patch management solutions provide controlled, secure, managed, and timely updates to systems and services. This is accomplished using a highly controlled public connection, leveraging a DMZ and zone-based architecture.

- **Network Maintenance Tools**: Systems and solutions that are used to facilitate centralized management and interrogation into the accurate and intended flow of data across and between networks, with particular attention to information support SLA management to both the LAN and the WAN providers.

GDIT's proposed solution includes a comprehensive set of network management tools to be located at each data center, and accessed remotely by the Needham, MA NSOC and all management facilities. Systems operate continuously to provide both real-time and historical understanding of the health of services and network conditions, and support the 24x7x365 nature of our operations environment.

GDIT has long and extensive experience designing data and voice networks to ensure a secure and defensible architecture. With network design and management contracts with the United States Marine Corps, the FAA, and other federal and state organizations, GDIT is uniquely qualified to provide the expertise necessary to plan and deploy a secure emergency communications network.

8.8.1. Environmental Requirements

Bidders shall describe in detail the environmental requirements of the system, including without limitation, space, power, heating, ventilation, and air conditioning (HVAC) requirements. The contractor shall provide to the State 911 Department the engineered BTU output and HVAC parameters for all CPE. The contractor shall provide cut sheets for all CPE furnished by the contractor at each PSAP.

Table 10 and Table 11 provide the environmental requirements (space/power/HVAC) for GDIT's proposed architecture at the data centers and PSAPs. GDIT's footprint at each data center consists of six cabinets, each 84'H x 24"W x 42"D. The total line-up utilizes 12 feet total end-to-end. Back-office equipment at the PSAPs will use a single enclosed cabinet with dimensions of 48'H x 24"W x 32"D for PSAPs sized between 1 and 5 positions and 84'H x 24"W x 42"D for PSAPs with 6 positions or more.

Table 10. Data Center Environmental Requirements

Equipment	Power (Watts)	HVAC (BTUs/Hr)
Cabinet #1 (84"H x 24"W x 42"D)		
Border Control	100 watts	342 BTU/Hr
Application Session Controller	3040 watts	10,384 BTU/Hr
Server Attached Storage	1200 watts	4100 BTU/Hr
Management/Functional Element Servers (i.e., ECRF, etc.)	4500 watts	15372 BTU/Hr
KVM	24 watts	82 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
Recorder	400 watts	1366 BTU/Hr
Cabinet #1 Total	**9424 watts**	**32,194 BTU/Hr**
Cabinet #2 (84"H x 24"W x 42"D)		
Customer Premise Equipment	22,806 watts	68,418 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
Cabinet #2 Total	**22,886 watts**	**68,966 BTU/Hr**
Cabinet #3 (84"H x 24"W x 42"D)		
Customer Premise Equipment	22,806 watts	68,418 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
Cabinet #3 Total	**22,886 watts**	**68,966 BTU/Hr**

Equipment	Power (Watts)	HVAC (BTUs/Hr)
Cabinet #4 (84"H x 24"W x 42"D)		
ESInet LAN/WAN	6810 watts	23,263 BTUs/Hr
EMC Storage	760 watts	2596 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
Cabinet #4 Total	**6970 watts**	**26,407 BTU/Hr**
Cabinet #5 (84"H x 24"W x 42"D)		
NTP	80 watts	274 BTU/Hr
Legacy Gateways	4000 watts	13,664 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
Cabinet #5 Total	**4240 watts**	**14,486 BTU/Hr**
Cabinet #6 (84"H x 24"W x 42"D)		
Legacy Gateways	5040 watts	17,220 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
Cabinet #6 Total	**5164 watts**	**17,768 BTU/Hr**

Table 11. PSAP Environmental Requirements

Equipment	Power (Watts)	HVAC (BTUs/Hr)
Small PSAP (2 – 5 Positions): Back-Office Equipment Suite Installed in Single Half Cabinet (48"H x 24"W x 32"D)		
ESInet LAN/WAN	300 watts	1026 BTU/Hr
Network Management	400 watts	1366 BTU/Hr
CAD Interface	1.5 watts	6 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
UPS	50 watts	171 BTU/Hr
NTP	40 watts	137 BTU/Hr
Recorder	400 watts	1366 BTU/Hr
Total	**1351.5 watts**	**4346 BTU/Hr**
PSAP (6 – 8 Positions): Back-Office Equipment Suite Installed in Single Full-Sized Cabinet (84"H x 24"W x 42"D)		
ESInet LAN/WAN	534 watts	1826 BTU/Hr
Network Management	800 watts	2732 BTU/Hr
CAD Interface	1.5 watts	6 BTU/Hr
Cabinet Fans	160 watts	548 BTU/Hr
UPS	50 watts	171 BTU/Hr
NTP	40 watts	137 BTU/Hr
Recorder	400 watts	1366 BTU/Hr
Total	**1985.5 watts**	**6786 BTU/Hr**
PSAP (9 – 14 Positions): Back-Office Equipment Suite Installed in Single Full-Sized Cabinet (84"H x 24"W x 42"D)		
ESInet LAN/WAN	444 watts	1518 BTU/Hr
Network Management	800 watts	2732 BTU/Hr
CAD Interface	1.5 watts	6 BTU/Hr
Cabinet Fans	150 watts	548 BTU/Hr
UPS	50 watts	171 BTU/Hr
NTP	40 watts	137 BTU/Hr
Recorder	400 watts	1366 BTU/Hr
Total	**1895.5 watts**	**6478 BTU/Hr**

Equipment	Power (Watts)	HVAC (BTUs/Hr)
PSAP (17 – 45 Positions): Back-Office Equipment Suite Installed in Single Full-Sized Cabinet (84"H x 24"W x 42"D)		
ESInet LAN/WAN	444 watts	1518 BTU/Hr
Network Management	800 watts	2732 BTU/Hr
CAD Interface	1.5 watts	6 BTU/Hr
Cabinet Fans	150 watts	548 BTU/Hr
UPS	50 watts	171 BTU/Hr
NTP	40 watts	137 BTU/Hr
Recorder	400 watts	1366 BTU/Hr
Total	**1895.5 watts**	**6478 BTU/Hr**
Call Taker Position Equipment Suite (Single Position)		
Flat Panel Display	43 watts	74 BTU/Hr
Workstation	240 watts	820 BTU/Hr
Audio Box	5 watts	18 BTU/Hr
UPS	50 watts	171 BTU/Hr
Printer	150 watts	513 BTU/Hr
Total	**488 watts**	**1596 BTU/Hr**

GDIT will provide complete and detailed engineered environmental requirement information and associated drawings for all data centers and PSAPs including floor plans, power, and HVAC information with engineered BTU output and HVAC parameters for all equipment in the system architecture. Additionally, GDIT will provide accurate cut sheets for all furnished CPE equipment at each PSAP.

8.8.2. Diagnostics

The system shall include built-in diagnostic software that shall automatically monitor alarm conditions of the equipment, applications, appliances, and services, and shall initiate audible and visual alarms and alerts in the event of any failure or disruption of the operations and/or processes and that shall include pro-active alerts for predictive failures. The State 911 Department reserves the right to request additional alarms.

The system shall alarm at the supervisor and administrative workstations (and other workstations identified by the State 911 Department in its sole discretion) and through other immediately recognized communications when the system is off line, and, where practicable, the system shall alarm at all PSAP positions.

The system shall include functionality that provides for automatic notification to the contractor's diagnostic repair center in the event of any failure or alert. Bidders shall identify all alarms reportable diagnostic anomalies, alarms, and alerts and shall state the frequency of review of such anomalies, alarms, and alerts.

Bidders shall define system diagnostic and normal tolerance practices and reports. The contractor shall maintain a daily report that logs alarms received by the system. The report shall be reviewed on a daily basis by the contractor's technical support staff as a preventive maintenance and proactive service log. The State 911 Department shall have on-line access to system report and logs, and the system shall have the ability to notify the State 911 Department via SMS, email, or other means requested by the State 911 Department.

The response shall include a listing of the system's standard alarms.

GDIT complies with the RFR specifications.

Our proposed diagnostic approach utilizes both proactive and reactive maintenance that is incorporated in our holistic network management approach. System-generated management traffic is a critical component of all monitoring, providing visibility into self-reporting and diagnostics for every system within the proposed solution. At minimum, all systems provide and report on systems' health and status, and self-reporting often includes detailed information on all

aspects of the systems and associated services, including event detail records, ingress traffic quality, payload specifications, and administrative access events. Management traffic will be (typically) placed into a management VLAN and transported (from PSAPs) over encrypted tunnels to surveillance systems within the Network and Security management 'block' within the data centers. These systems continually collect, analyze, and monitor traffic, and provide real-time and historical reporting of a range of (configurable) performance and health parameters. This information is used to provide reporting to the Commonwealth, combined with application specific reports.

Each ESInet functional system will be configured in the types and structure of reported management data, to include alarms based on severity levels. In addition to the functional ESInet applications, network infrastructure and monitoring systems will survey traffic based on policy and report on these parameters. This includes the use of all edge routers for performing security inspection, the use of TACACS to monitoring switch ports, and the use of packet capture probes (Oracle Palladion) to report on QoS. Each identified component will be configured to report alarms based on configurable crossing thresholds, and alarms will be reported on surveillance systems to allow for reactive maintenance.

Of particular note in GDIT's network management construct is the importance of augmenting reactive monitoring with proactive maintenance. Due to the transient nature of converged services, proactive maintenance is a critical component of the future reliability model by identifying network congestion, contention, and performance issues through trend analysis before they become detrimental to services (causing alarms). In this regard, packet inspection is vastly superior to end-point reporting techniques, such as Real Time Control Protocol (RTCP). Packet inspection is performed in the GDIT solution by the Oracle Palladion probe placed at each site, providing in-depth knowledge of both media (payload) and the associated signaling (control) traffic. It is important to associate media with signaling so that data is logged and saved for every emergency services incident, and so that performance and media quality statistics are presented to administrators for detailed diagnostics and event management.

GDIT's proposed solution has specified the SolarWinds Orion platform as the network management surveillance system. The Orion solution offers multiple software applications integrated together to provide a comprehensive monitoring solution that analyzes and reports on the status of all systems, applications, appliances, and services with automated alerting functionality through configurable audible and visual means in the event a failure or disruption of operations is detected. The alarm functionality is user configurable based on pre-established thresholds, so additional alerts can be configured and added as requested.

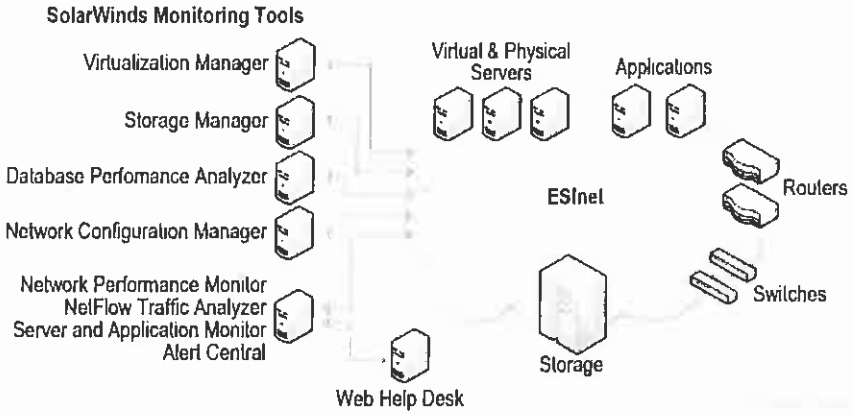


Figure 58. NG9-1-1 System Monitoring

The SolarWinds platform comprises the following capabilities:

- **Network Performance Monitor** – SolarWinds Network Performance Monitor (NPM) detects, diagnoses, and resolves performance issues before outages occur. This easy-to-use agentless software delivers real-time views and dashboards that enables visual tracking and monitoring of network performance. NPM provides dynamic network topology mapping and automated network discovery.

- **Netflow Traffic Analyzer** – SolarWinds NetFlow Traffic Analyzer (NTA) enables administrators to capture data from continuous streams of network traffic and convert those raw numbers into easy-to-interpret charts and tables that quantify exactly how the network is being used, by whom and for what purpose.

- **Server and Application Monitor** – SolarWinds Server & Application Monitor provides agentless application and server monitoring software for alerting, reporting, and server management. This monitoring software supports multiple hardware vendors along with the underlying hardware for VMware® hosts. Server & Application Monitor provides built-in support for more than 150 applications and additional custom application monitors can be created in minutes. Server management and remediation capabilities allow administrators to start and stop services, reboot servers, and kill rogue processes.

- **Network Configuration Manager** – SolarWinds Network Configuration Manager (NCM) simplifies the management of configuration files for network devices. NCM provides central management of multi-vendor devices from a single intuitive, point-and-click web console. NCM provides automated network configuration backups, bulk change deployment, real-time change alerts, detailed inventory lists, and compliance reporting.

- **Database Performance Analyzer** – Database Performance Analyzer focuses on instance response time, finding the root causes of delays inside of database servers. It tracks every query in every session, and captures the server wait types that impose delays on the query. Database Performance Analyzer correlates other essential statistics to give a complete understanding of performance problems.

- **Storage Manager** – SolarWinds Storage Manager provides monitoring on the performance and capacity of end-to-end physical and virtual storage infrastructure. Storage Manager monitors storage performance and isolates hotspots in your multi-vendor storage solutions, maps virtual machines to physical storage, automates storage capacity planning and reporting, and simplifies analysis of storage usage and reclamation of storage space.

- **Virtualization Manager** – SolarWinds Virtualization Manager provides integrated VMware and Microsoft Hyper-V capacity planning, performance monitoring, VM sprawl control, and configuration management. Real-time dashboards simplify the identification and troubleshooting of performance, capacity, and configuration problems. Virtualization Manager identifies VM sprawl, helps to reclaim and optimize space, and reduces potential licensing costs. It seamlessly integrates with SolarWinds Server & Application Monitor to provide application management from the application to datastore.

- **IP Address Manager** – SolarWinds IP Address Manager (IPAM) simplifies IP address management and DHCP and DNS administration. SolarWinds IPAM offers centralized IP address management with unified DHCP and DNS administration to easily find available IP addresses, automatically configure DHCP and DNS settings, and publish accurate address documentation. In addition, it actively monitors critical IP resources like DHCP scopes and available active IP addresses, and it configures and receives alerts and reports.

- **Web Help Desk** – SolarWinds Web Help Desk (WHD) creates a structured, consistent system for help desk processes and communications. WHD integrates seamlessly with other SolarWinds applications, enabling WHD to open tickets automatically based on SolarWinds alerts. WHD discovers and synchronizes asset information when triggered, or automatically, when scheduled. With the ability to integrate with other SolarWinds applications, WHD enables easy discovery and import of asset data. WHD automatically sends trouble ticket emails when a ticket is opened, escalated, updated, or closed. Ticket generation and updates can be accomplished by sending an email to the WHD system. WHD then takes predefined actions based on the email content. Predetermined procedures can be set for each step of the ticket process from origination, dispatch, parts ordering, and escalation through to closure, ensuring consistent service. WHD contains a change approval process, including roles for submitters and multiple levels of approvers.

- **Alert Central** – SolarWinds Alert Central is centralized IT alert management software that provides alert management. It consolidates and manages IT alerts, alert escalation, and on-call scheduling to help ensure all alerts get to the right technician, in the right groups, at the right time.

SolarWinds provides for the configuration of alerts to any authorized supervisor or administrator through email and SMS text messaging. GDIT will work with the State 911 Department to identify the appropriate personnel to receive notification depending on criticality and configure the system to automatically generate alarms to these individuals when the condition arises.

As described above, the SolarWinds platform will automatically generate notification of events based on pre-determined workflows. At all times, NSOC administrator will have immediate 24x7 visibility into open tickets and can manually escalate priority as required. GDIT will work with

the State 911 Department to provide minimum escalation periods of outages based on the criticality of the system outage.

GDIT will establish work procedures for NSOC personnel that will include the requirement for NSOC management to review alert logs on a daily basis and provide reports that detail the status of all open alarm conditions. In the event trouble tickets remain active for longer than predetermined intervals, addition information will be provided that elaborates on the reason for delay in resolution and current strategy for final resolution in a timely fashion. Reports will be made available to the State 911 Department through an online web portal and can be provided by other means as requested.

SolarWinds has default predefined alerts that assist in quickly enabling operations. Table 12 lists those alerts for the monitoring applications listed above.

Table 12. List of the System's Standard Alarms

Network Performance Monitor Predefined Alerts	
Alert when a node or group goes down	Alert when a node reboots
Alert when an interface is shut down	High Physical Memory Utilization with Top 10 Processes
Alert when a node is deleted	Alert on Cisco IOS version or IOS image family change
Alert when a group goes into a warning or critical state	Alert when a polling engine has not updated the database in 10 minutes
Alert when any hardware component goes into a warning or critical state	Alert when a node, interface, wireless access point, or group goes down
Alert when a multicast routing group goes down	Alert when a node reboots
Alert when a multicast routing group has different status from normal	Alert when a device experiences high CPU utilization, high packet loss, high response time, high receive percent utilization, or high transmit percent utilization
Alert when multicast routing group traffic is lower than a specified value	Alert when a managed node has not been polled during the last 5 tries
Alert when multicast routing group traffic is lower than a specified value	Alert when a polling engine has not updated the database in 10 minutes
Alert when a managed node last poll time is 10 minutes old	Alert when a rogue access point is detected
Alert when a managed node has not been polled during the last 5 tries	Alert when a wireless access point has more than 10 clients
Netflow Traffic Analyzer Predefined Alerts	
Top Talker Alerts	**CBQoS Alerts**
High Receive Percent Utilization with Top Talkers	Pre-Policy
High Transmit Percent Utilization with Top Talkers	Post-Policy
	Drops
Database Performance Analyzer Predefined Alerts	
Total database instance wait time	SQL Server abnormal mirroring status
Total SQL wait time for a single SQL	SQL Server error log alert
Average wait time for a single SQL	SQL Server ineffective statistics
Total SQL wait time for a single wait	SQL Server job failure
Total SQL wait time for a program	SQL Server log has many virtual logs
Total SQL wait time for a database user	SQL Server long running jobs
Total SQL wait time for a machine	Concurrent sessions
Total SQL wait time for a database	Locking – repository
Total blocking wait time	Locking – instance

Database instance availability	Disk space monitor
Database frees pace	Job failure
Database instance parameter changes	CPU utilization
Transaction log free space	Procedure cache hit ratio
Database Performance Analyzer database instance monitor errors	SQL agent service status
Database Performance Analyzer resource collection errors	Plan changes
Windows service not running	Fragmentation
Virtualization Manager Predefined Alerts	
VM – No heartbeat	VM Storage Rightsize
Datastore high I/O delay	VMs with Large Snapshots
VM Memory Limit Configuration	VMs with More Allocated Space than Used
High VM Memory Utilization	VMs with Connected Media
Host memory utilization	Cluster predicted CPU depletion
Hosts rebooted	VM CPU Underallocated
Hosts – No heartbeats	VM Memory Overallocated
VM memory swap	Cluster predicted memory depletion
High VM CPU Utilization	VM CPU Overallocated
Host Network Utilization High	VMs with Old Snapshots
VM CPU ready	Datastore low free space
VM memory ballooning	VM Phantom Snapshot Files
Cluster storage utilization	Hosts – No BIOS ID
Host console memory swap	Zombie VMs
Cluster CPU utilization	Datastore Overallocation
Host CPU utilization	Disk 100% within the week
Guest storage space utilization	VMs with Bad Tools
VMs rebooted	Stale VMs
Host bus resets	VM disk near full
VM Potential Unused CPU	Inactive VMs – disk
VM Disk Latency	VM Memory Underallocated
Host Command Aborts	Cluster low VM capacity
Cluster memory utilization	Host partition storage free space
Host to datastore latency	Cluster predicted disk depletion
Datastore Excessive VM Log Files	
IP Manager Predefined Alerts	
High DHCP Scope Usage Monitoring	High Subnet Usage Monitoring
Notes: *Server and Application Monitor provides only custom advanced alerts* *Network Configuration Manager provides additional configuration detail to alerts in Network Performance Monitor* *Storage Manager provides only custom advanced alerts*	

8.8.3. Self-Monitoring

The system shall include a self-monitoring function of monitoring vital processes and sending alarms in the event of an alarm condition. The system shall notify the communications supervisor, local system administrator, and/or local maintenance personnel upon detection of an alarm.

GDIT will comply with the RFR specification.

As described previously in detail in Section 8.8.2 (Diagnostics), GDIT's solution includes a comprehensive system monitoring capability that includes capability to monitor all vital

processes of the NG9-1-1 system that will provide and comply with the RFR specifications. The system also provides the capability to define alarm conditions and thresholds based and a broad range of system information. The alerting functionality includes the capability to define personnel to receive these alarms based on alarm criteria and criticality. The solution provides a centralized platform that maintains current status of open alerts, and all NG9-1-1 operations personnel will have access to the system.

8.8.4. System Health Monitoring

The system shall include a health monitoring function that shall monitor the functioning of the system. The system shall be able to produce ad hoc reports of system functioning, and the State 911 Department shall have read-only access to such reports. Bidders shall specify a schedule by which proactive testing shall be performed to ensure the continued health of the system.

GDIT will comply with the RFR specification.

Section 8.8.2 (Diagnostics) of this proposal provides a detailed description of the monitoring system provided with our solution. SolarWinds Network Performance Monitor and Server & Application Monitor provide an integrated capability to monitor the health of all system components including network devices, appliances, servers, operating systems, and applications. Database Performance Analyzer, Storage Manager, and Virtualization Manager provide additional capabilities to provide detailed health information of specific components within the NG9-1-1 system.

System health reports can be generated by a couple of sources depending on the nature of the report. The Oracle Enterprise Operations Monitor provides reporting capability on call processing operations of the NG9-1-1 system (additional information in Section 8.8.7, Operational Reporting). Using a Crystal Reports capability, ad hoc reports can be generated from Oracle DataSource to generate any type of report required by the Commonwealth. Additionally, the SolarWinds management platform provides the capability of providing reports based on a host of information gathered across the various components monitored. SolarWinds has a host of predefined reports and the capability of defining customized reports at the user level on any information collected by the integrated SolarWinds platform.

The GDIT solution provides an external-facing web portal that will consolidate reporting information in web format for access by Commonwealth personnel. Utilizing the remote access capability of the system (see Section 8.8.5, Remote Access), Commonwealth personnel will log into the web portal and, depending on credentials, may be limited to read-only access to the reports provided.

GDIT NSOC operators will conduct regular system health testing at intervals coordinated with the State 911 Department, but no less frequently than monthly. Reports will be generated and provided to Commonwealth personnel. Reports will be analyzed over time to evaluate trend data of the system over time to assist in proactively predicting preventive maintenance or replacement of components.

8.8.5. Remote Access

The response shall define how secure remote access to any or all components of the system is achieved, including security of such access. The State 911 Department shall have remote read-only access to all components of the system.

Our proposed secure Remote Access capability fully complies with the RFR specifications. Figure 59 shows the components that make up GDIT's secure remote access capability.

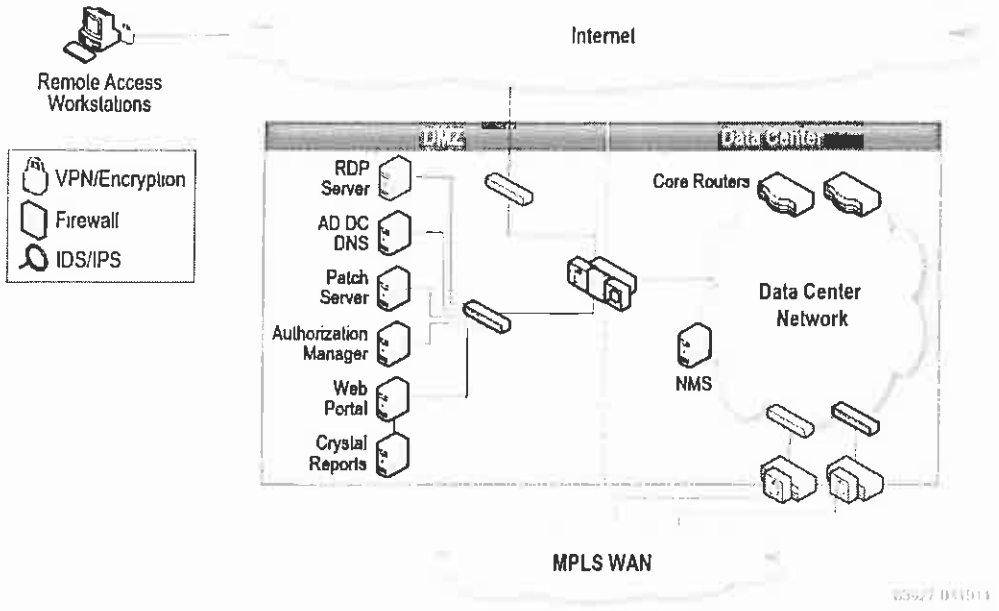


Figure 59. Secure Remote Access

- **Authentication Manager** – The Authentication Manager server provides authentication service for RSA Smart Tokens, which will be provided to all remote users requiring any type of remote access to the NG9-1-1 system. These tokens provide for secure two-factor authentication to the network. Once authenticated, a client VPN session is established to the firewall/VPN connected to the external Internet connection point.

- **Active Directory Domain Controller** – The domain controller in the DMZ is a secondary read-only instance of the NG9-1-1 AD domain. This domain controller is used to authenticate services for remote users to internal resources. Commonwealth personnel will have limited read-only access to resources. Remote administrators and service technicians will have additional access privileges to provide access to necessary internal resources to perform required administrative duties.

- **Web Portal** – The web portal will provide access to web-based reports for external users. As required, reports will be generated by NSOC personnel and or automatically by monitoring systems and stored on the web portal for presentation to Commonwealth personnel.

- **Crystal Reports** – Crystal Reports provides the capability for users to create their own reports from datastores residing on various management systems within the NG9-1-1 system. See Section 8.8.4 (System Health Monitoring) for further details.

- **RDP Server** – The Remote Desktop Protocol (RDP) server provides the capability for administrators to access internal devices for the purpose of management and

administration. Rather than opening administrative sessions from any location on the Internet, this server will be the only device allowed through the boundary of the data center. Administrators will make a remote session to this device and then this device to internal devices. Only NG9-1-1 administrators will be allowed access to this server.

- **Patch Server** – The Patch Server will provide a gateway for the reception of vendor software and signature updates. This central repository will be evaluated for security and configuration control prior to deployment into the NG9-1-1 system (see Section 8.11, Security, Anti-Virus, and Patch Management).

8.8.6. Alarm Categories

The system shall include categories of alarms for, at a minimum, each of the event types (catastrophic, major, and high priority, standard priority system malfunctions) depending on the criticality of the event. The system should allow the administrator to configure notification thresholds. In addition to these alarm categories, the contractor shall, at the request of the State 911 Department, create new alarm categories.

The system shall send notifications of alarm conditions to communication supervisors and maintenance personnel in the manner specified by the State 911 Department and on a distribution list as specified by the State 911 Department. The notification shall summarize the SNMP trap that triggered the alarm condition.

Our proposed system fully complies with the RFR specifications; includes all specified ;; and also allows the creation of Additionally, our solution is capable of sending any specified personnel or agencies.

GDIT's network management solution is also further detailed in Section 8.20.7.3 (Network Security and Operations Center) and Section 8.20.9 (Monitoring of Applications, Appliances, and CPE).

8.8.7. Operational Reporting

The response shall include a description of the comprehensive management and statistical reporting functionality that will provide the State 911 Department and/or PSAP management personnel with real-time and historical records. The system's operational reporting shall be user friendly, customizable, and capable of generating reports for varying time periods, from one or all PSAPs cumulatively, including without limitation, ad hoc reports and to run reports as needed. The system shall have browser-based capabilities for ease of remote access. The retention period for such historical records shall be a minimum of three (3) years. The system also shall be able to auto-schedule the generation of predefined ad hoc reports.

At a minimum, the following data elements shall be readily available for reporting purposes at the system level and at the PSAP level:

A. Payload processing times;

B. Seizure time;

C. Position answered;

D. Answer time;

E. Disconnect time;

F. Incoming IP address;

G. Total count of Payloads by Type;

H. Average Event Waiting Report;

I. Average Event duration;

J. Total Abandoned Events;

K. Events by incoming IP address;

L. Events by hour of day;

M. Events answered by position;

N. Events answered by all positions;

O. Events answered by user ID;

P. Events by day of the week;

Q. Events transferred;

R. Agent availability report;

S. Call volumes;

T. Individual Call Information;

U. Collection of Calls;

V. Summary of Call Loads;

W. Total number of wireless and wireline 911 calls answered by wireless state police PSAPs, by PSAP, by cellular sector, wireline only, wireless only;

X. Total number of wireless and wireline 911 calls transferred from the wireless state police PSAPs to the local PSAPs, by PSAP, by cellular sector, wireline only, wireless only;

Y. Total number of wireless and wireline 911 calls transferred from the local PSAP, location to which call was transferred, type of entity to which call was transferred, and percentage of each type of entity to which call was transferred, by PSAP, by cellular sector, wireline only, wireless only; and

Z. Total number of simultaneous wireless and wireless 911 calls per day, week, month, and year, and the number of occurrences, and the dates(s) of occurrence, by PSAP, by cellular sector, wireline only, wireless only.

The response shall describe, and provide examples of, standard individual workstation reports generated by the CPE regarding individual calls, collection of calls and call volumes, summary of call loads, and other pertinent information gathered by the CPE.

GDIT's fully compliant Operational Reporting system includes an easy-to-use real-time comprehensive management and statistical reporting capability.

GDIT has designed a robust reporting solution that meets the requirements of the Commonwealth. The bulk of the reports are natively produced from either the Palladion management solution and/or the IP ACD call taking system: ECW's CallStation. Many of the reports listed have to do with call flow, call quality, and call type statistics traditionally found within Call Detail Records (CDR). The Border Control Function (BCF) is the Oracle session border controller with call detail reporting provided by Oracle's Palladion product. GDIT's solution also provides Palladion probes at each of the PSAPs to ensure our solution can monitor call quality and call details from entry into the ESInet to the PSAP.

Oracle's Palladion is a proven state-of-the-art management platform that provides dashboard performance and reporting capabilities (see Figure 60).

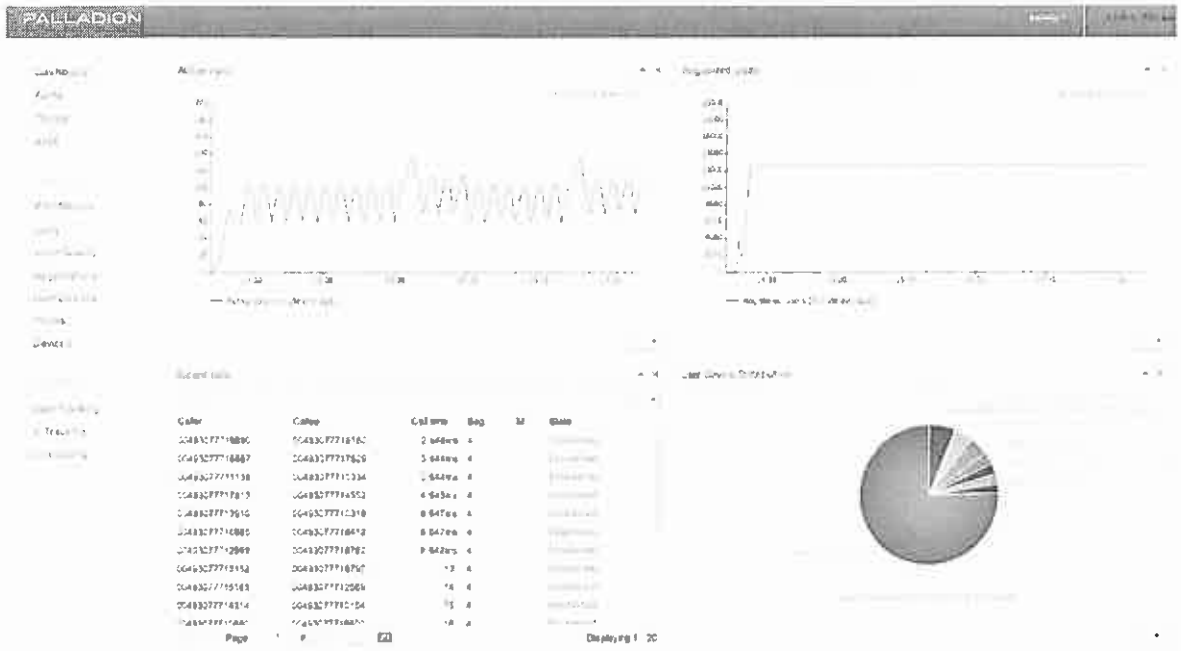


Figure 60. Palladion Performance and Reporting Dashboard

Figure 60 is a sample Palladion dashboard configuration for Active Calls, Registered Users, and Recent Calls with a graphic that depicts distribution of calls. The dashboard functionality within Palladion is customizable.

The Palladion reporting capabilities also provide statistics and reports related to call quality. A sample report depicting call quality is shown in Figure 61.

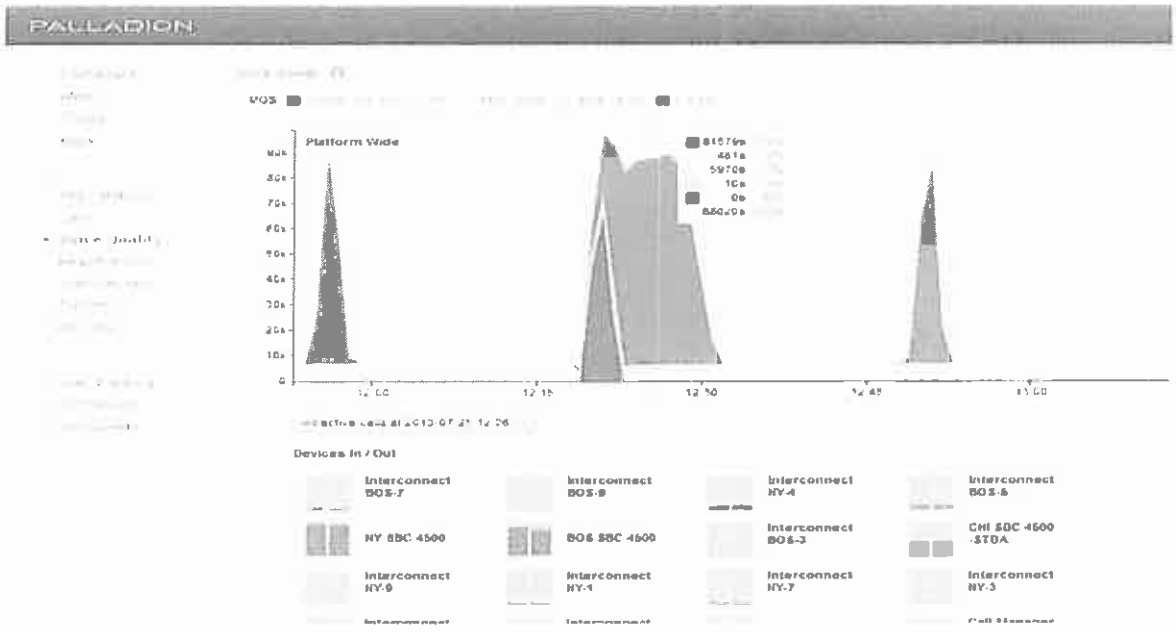


Figure 61. Palladion Call Quality Sample Report

Additional operational reporting capabilities will be provided by the IP ACD call taking CPE solution provided by Emergency CallWorks (ECW).

The CPE solution provides a comprehensive management and statistical reporting system to provide PSAP management personnel with real-time and historical information. The reporting system is customizable and capable of generating reports for varying time periods. 9-1-1 Call Detail Reports include ANI, ALI, seizure time, position answered, answer time, transfer time, disconnect time, incoming trunk number, and more. The CPE call taking solution stores all data into a unified database backend. This includes all Call state information, ALI information, etc. The Management Information System (MIS) accesses this backend database directly and, therefore, provides the Commonwealth access to live data and events as it occurs in real-time. All reports and statistics include currently active calls in the system and provide the ability to setup report time frames down to the minute for all available reports.

Standard reports with pre-defined time window parameters can be automatically exported to PDF and emailed to a defined list of recipients. The CPE solution also provides access to reports via WebAccessory in which authorized users can monitor live operations (calls and incidents), view canned reports, and perform ad-hoc database queries among other tasks. Figure 62 through Figure 67 provide sample workstation-generated reports regarding individual calls, collection of calls, call volumes, and summary of call loads as well as other pertinent sample reports.

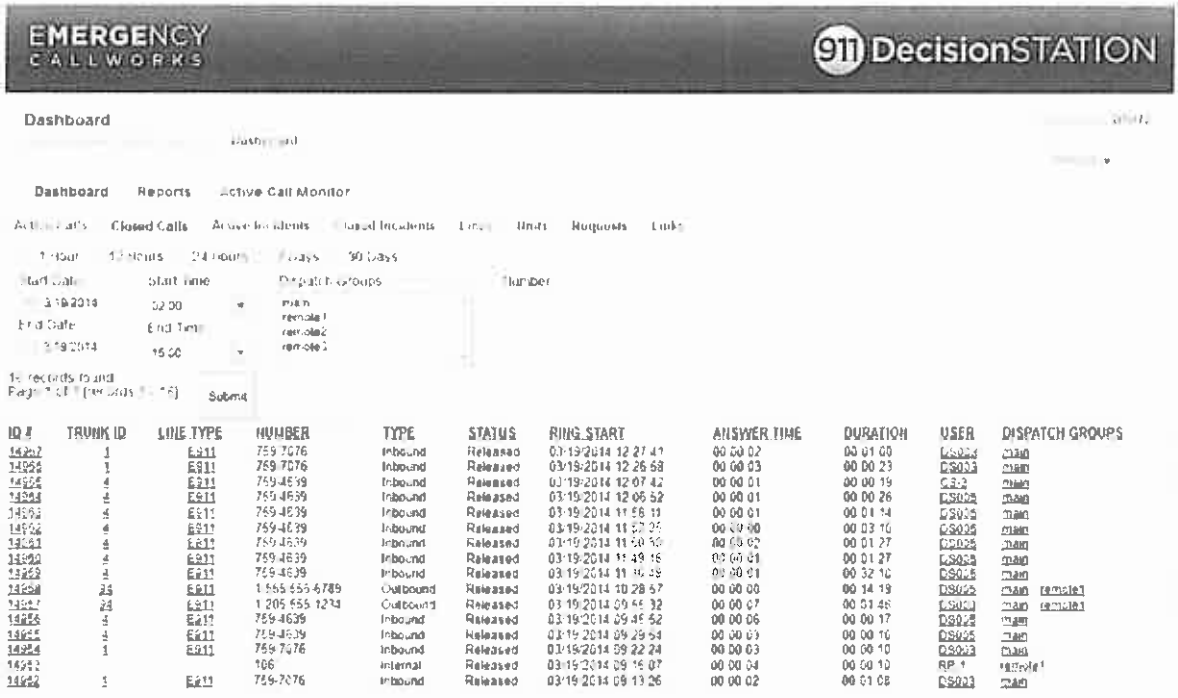
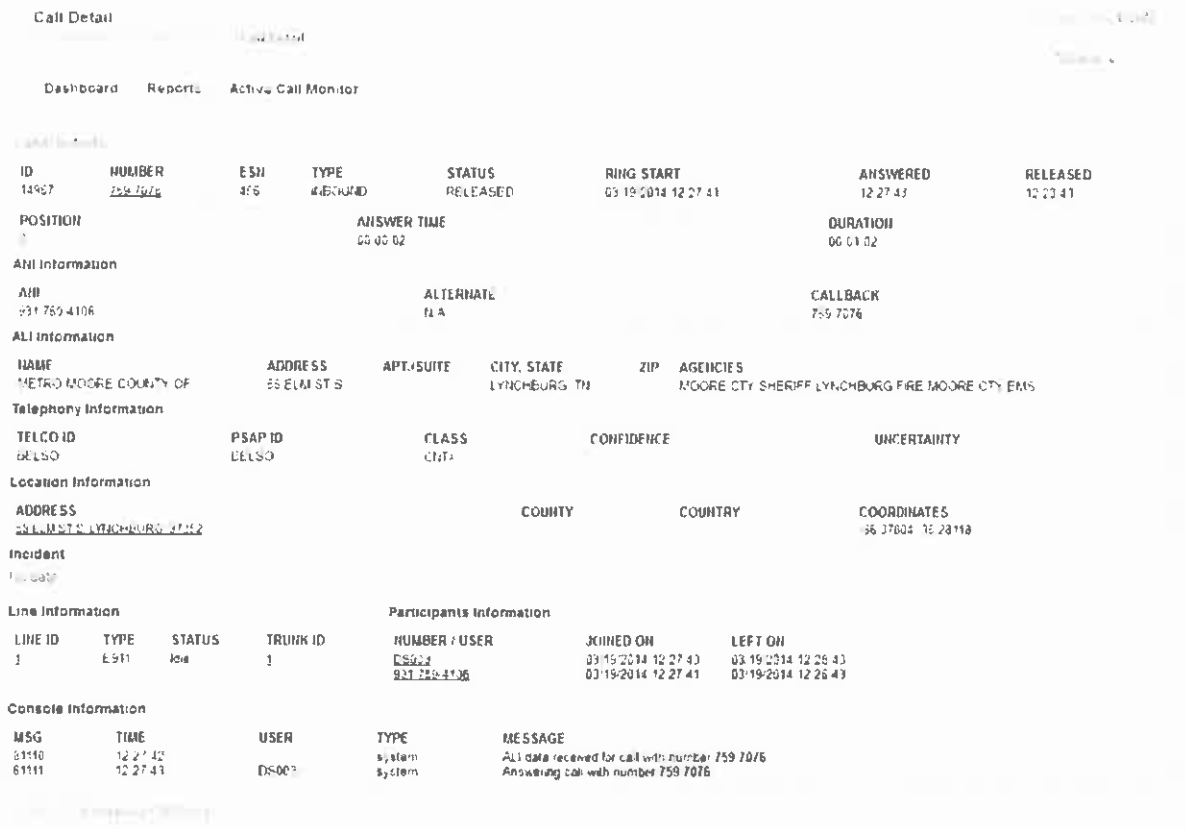


Figure 62. Individual Calls


Call Detail

Dashboard Reports Active Call Monitor

ID	NUMBER	ESN	TYPE	STATUS	RING START	ANSWERED	RELEASED
14967	759 7076	456	INBOUND	RELEASED	03/19/2014 12:27:41	12:27:43	12:28:41

POSITION	ANSWER TIME	DURATION
1	00:00:02	00:01:02

ANI Information

ANI	ALTERNATE	CALLBACK
931 759 4106	N/A	759 7076

ALI Information

NAME	ADDRESS	APT/SUITE	CITY, STATE	ZIP	AGENCIES
METRO MOORE COUNTY GF	55 ELM ST S		LYNCHBURG TN		MOORE CTY SHERIFF LYNCHBURG FIRE MOORE CTY EMS

Telephony Information

TELCO ID	PSAP ID	CLASS	CONFIDENCE	UNCERTAINTY
DELSO	DELSO	CNTA		

Location Information

ADDRESS	COUNTY	COUNTRY	COORDINATES
55 ELM ST S LYNCHBURG 37352			35.37604 -86.38118

Incident

No data

Line Information

LINE ID	TYPE	STATUS	TRUNK ID
1	E911	Idle	1

Participants Information

NUMBER / USER	JOINED ON	LEFT ON
DS003	03/19/2014 12:27:43	03/19/2014 12:28:43
931 759 4106	03/19/2014 12:27:41	03/19/2014 12:28:43

Console Information

MSG	TIME	USER	TYPE	MESSAGE
61110	12:27:42		system	ALI data received for call with number 759 7076
61111	12:27:43	DS003	system	Answering call with number 759 7076

Figure 63. Call Detail Record

9-1-1 Calls by Class of Service

ECX Test Network #1

Start Date 2013-10-01 Shift Start 08:00

End Date 2013-11-01 Shift End 18:00

Dispatch Groups main, remote1, remote2, remote3

Class of Service	Answered Calls	Abandoned Calls	Total Calls	% of Total	% Wireless
BUSN	534	1	535	13.61%	
CNTX	1684	22	1706	43.39%	
MOBL	1	0	1	0.03%	0.03%
PBXB	142	0	142	3.61%	
RESD	1050	8	1058	26.91%	
Unknown	478	1	479	12.18%	
VOIP	1	0	1	0.03%	
WPH1	1	0	1	0.03%	0.03%
WPH2	5	1	6	0.15%	0.15%
WRLS	3	0	3	0.08%	0.08%
Total	3899	33	3932	100.00%	0.28%

Thu, 7 Nov 2013 09:48:41 DS372 Page 1 of 1

Figure 64. Call Type Report by Class of Service

Calls by Call Type

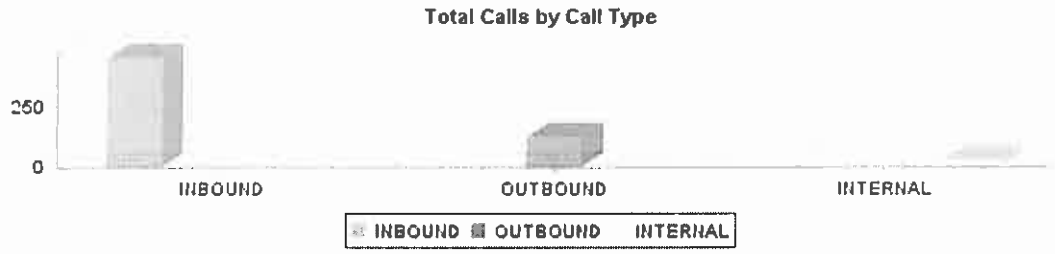
ECX Test Network #1

Start Date 2013-09-01 Shift Start 08:00 User –

End Date 2013-09-30 Shift End 18:00

Dispatch Groups main, remote1, remote2, remote3

	Inbound		Outbound		Internal		Total	
	Calls	Avg Call Duration	Calls	Avg Call Duration	Calls	Avg Call Duration	Calls	Avg Call Duration
9-1-1	455	04:48.2					455	04:48.2
7-Digit	1	01:11.0					1	01:11.0
Admin			124	03:00.2	31	01:03.7	155	02:36.9
Total	456	04:47.3	124	03:00.2	31	01:03.7	611	03:57.5



Mon, 28 Oct 2013 10:03:49 DS372 Page 1 of 1

Figure 65. Collection of Calls – By Call Type

Calls by Hour and Day

ECX Test Network #1

Start Date 2013-10-01

End Date 2013-11-01

Queues --

Hour	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Total	% Total	Avg	Med
00 00 - 01 00	0	0	0	0	0	0	0	0	0 00%	0	0
01 00 - 02 00	0	0	0	0	0	0	0	0	0 00%	0	0
02 00 - 03 00	0	0	0	0	0	0	0	0	0 00%	0	0
03 00 - 04 00	0	0	0	0	0	0	0	0	0 00%	0	0
04 00 - 05 00	0	0	0	0	0	0	0	0	0 00%	0	0
05 00 - 06 00	0	0	0	0	0	0	0	0	0 00%	0	0
06 00 - 07 00	0	0	0	0	0	0	0	0	0 00%	0	0
07 00 - 08 00	0	0	0	0	0	0	0	0	0 00%	0	0
08 00 - 09 00	0	0	21	2	6	9	0	38	0 41%	5	2
09 00 - 10 00	0	3	36	1,853	7	11	0	1,910	20 39%	273	7
10 00 - 11 00	0	8	8	11	9	2	0	38	0 41%	5	8
11 00 - 12 00	0	2	8	9	17	1	0	37	0 39%	5	2
12 00 - 13 00	0	0	5	4	6	4	0	19	0 20%	3	4
13 00 - 14 00	0	4	2	10	2	3	0	21	0 22%	3	2
14 00 - 15 00	0	27	8	11	1,009	36	0	1,091	11 64%	156	11
15 00 - 16 00	0	11	6	11	9	895	0	932	9 95%	133	9
16 00 - 17 00	0	18	928	18	3,201	871	0	5,036	53 75%	719	18
17 00 - 18 00	0	1	220	12	10	4	0	247	2 64%	35	4
18 00 - 19 00	0	0	0	0	0	0	0	0	0 00%	0	0
19 00 - 20 00	0	0	0	0	0	0	0	0	0 00%	0	0
20 00 - 21 00	0	0	0	0	0	0	0	0	0 00%	0	0
21 00 - 22 00	0	0	0	0	0	0	0	0	0 00%	0	0
22 00 - 23 00	0	0	0	0	0	0	0	0	0 00%	0	0
23 00 - 24 00	0	0	0	0	0	0	0	0	0 00%	0	0
Total	0	74	1,242	1,941	4,276	1,836	0	9,369			
% Total	0 00%	0 79%	13 26%	20 72%	45 64%	19 60%	0 00%				
Average	0	3	52	81	178	76	0				
Median	0	0	0	0	0	0	0				

Wed, 6 Nov 2013 09 20 54 CS372 Page 1 of 1

Figure 66. Call Volumes – By Hour and Day

Call Summary

ECX Test Network #1

Start Date 2013-11-01 Shift Start --

End Date -- Shift End --

Dispatch Groups --

Call Type	# Calls
9-1-1 Calls	10
Answered 9-1-1 Calls	9
Abandoned 9-1-1 Calls	1
7-Digit Emergency Calls	0
Admin Calls	0
Answered Admin Calls	0
Abandoned Admin Calls	0
Outbound Calls	1

Mon, 4 Nov 2013 14:05:59 DS072 Page 1 of 1

Figure 67. Summary of Call Loads

Table 13 provides further summary details of which solution will provide each report as stated within this Operational Reporting section.

Table 13. Report Type and Reporting Solutions

Report Type	Reporting Solution
Payload processing times	Palladion
Seizure time	Palladion
Positioned Answered	ECW
Answer Time	ECW
Disconnect time	ECW or Palladion
Incoming IP Address	Palladion
Total count of payloads by type	ECW
Average Event Waiting Report	ECW
Average Event duration	ECW or Palladion
Total Abandoned Events	Palladion
Events by incoming IP Address	Palladion
Events by hour of day	Palladion
Events answered by position	ECW
Events answered by all positions	ECW
Events answered by User ID	ECW
Events by day of the week	ECW and Palladion
Events transferred	ECW
Agent availability report	ECW
Call volumes	ECW and Palladion
Individual Call Information	ECW
Collection of Calls	ECW and Palladion
Summary of Call Loads	ECW
Total number of wireless and wireline 9-1-1 calls answered by wireless state police PSAPs, by PSAP, by cellular sector, wireline only, wireless only	ECW
Total number of wireless and wireline 9-1-1 calls transferred from the wireless state police PSAPs to the local PSAPs, by PSAP, by cellular sector, wireline only, wireless only	ECW
Total number of wireless and wireline 9-1-1 calls transferred from the local PSAP, location to which call was transferred, type of entity to which call was transferred, and percentage of each type of entity to which call was transferred, by PSAP, by cellular sector, wireline only, wireless only	ECW
Total number of simultaneous wireless and wireless 9-1-1 calls per day, week, month, and year, and the number of occurrences, and the dates(s) of occurrence, by PSAP, by cellular sector, wireline only, wireless only	ECW

Additionally, all maintenance logs, statistics, call records, ALI information, and TDD/TTY conversations have the ability to be saved in electronic format. The data generated from these reports is exportable to "off-the-shelf" database or reporting software, including Crystal Reports.

GDIT's reporting solution also includes Crystal Reports 2013 to enable the Commonwealth to utilize data sources from the ESInet call flow elements to develop and automate customized reports.

8.9. PROJECT MANAGEMENT

Bidders shall describe in detail the project management, staffing and planning functions. The contractor shall provide for project management to ensure a satisfactory implementation. Staffing for project management shall include, at a minimum, one designated project manager responsible for oversight, management, and supervision, and status reporting of their own technical personnel involved in the provisioning activities. Project managers shall have substantial experience working on large scale, integrated public safety technology implementations. The contractor's proposed candidates for project management positions shall be approved by the State 911 Department.

The contractor shall be subject to and shall provide project management in accordance with the Commonwealth's project management methodology known as Commonway Project Management Methodology. Information regarding the Commonway Project Management Methodology is available at www.mass.gov/itd.

All written documents shall be delivered in machine-readable format, capable of being completely and accurately reproduced by computer software on a laser printer. All itemized and/or annotated lists shall be delivered in computer spreadsheets, capable of being imported to Microsoft Excel 2007 or higher. All meetings shall be held at the offices of the State 911 Department, unless agreed to otherwise by the State 911 Department.

The contractor represents and warrants to the State 911 Department that the contractor shall be sufficiently staffed and equipped to fulfill contractor's obligations under the contract, contractor's services shall be performed by appropriately qualified and trained personnel, with due care and diligence and to a high standard of quality as is customary in the industry, in accordance with the terms and conditions of the contract and in accordance with all applicable professional standards.

The contractor shall ensure that appropriate organizational management has authority to exercise decision-making over contractual matters, and the contractor shall escalate such matters to the appropriate organizational level.

GDIT will comply with the RFR specification.

As our core business is telecommunications and IT systems integration, our team's strength is project management and engineering. Our existing Project Management team consists of highly experienced professionals, most of whom have more than 20 years of experience in the field and many with Project Management Professional (PMP) certifications. Table 14 shows some of our current team member's experience and their roles within the MA NG9-1-1 project.

Table 14. GDIT MA NG9-1-1 Project Team Experience

Name	Role	PMP Certification	Years with GDIT	Years in Telecom/IT
Joan Newlon	Project Director		30	20
Peter Joo	Engineering Director		17	37
Paul Brillaud	Systems Architect & Engineering Manager		5	25
Paul Chotkowski	Senior Project Manager	Yes	11	32
Ted Gausmann	Network Operations Center (NOC) Manager		22	18
James Dionne	Project Management	Yes	10	35
Joseph Navarro	Test and Certification Manager	Yes	8	28
Jeff Modica	Field Implementation Manager		19	18

As introduced in Section 8.1 (Project Overview), GDIT will utilize established best practices and a highly regimented *integrated management approach* for the Commonwealth of Massachusetts NG9-1-1 project. GDIT's project management approach uses the CommonWay project management methodology and with each life cycle phase tightly integrated with the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK). The GDIT team's management framework is based on industry best practices, and includes ISO 9001 and ISO 20000-registered processes. These processes are documented in our Quality Management System (QMS), and provide a **foundation for effective project management**:

- Improve overall project performance
- Increase projects delivered on-time and within budget
- Reduce project risk
- Enhance quality
- Improve inter- and intra-project communication
- Establish a consistent standard that everyone can follow
- Complement standard System Development Life-Cycle Methodologies (SDLC)
- Utilities a common project management terminology

Our processes are fully compliant with the CommonWay methodology, and we will adapt our templates where needed to provide any unique information requested for the Commonwealth's specific requirements. Mr. Paul Chotkowski is designated as the Project Manager, who is responsible for oversight, management, supervision, and status reporting for the project.

Table 15. Program Management Processes and Tools. The GDIT team's program management processes and tools are the foundation for effective project management and efficient technical activities.

Features of GDIT's Processes and Tools	Benefits to the Commonwealth
A repeatable set of processes for use by Project Managers and Technical Leads	Operational efficiency and overall quality performance
Allows our team to distill best practices and lessons learned from their programs	Experience-based processes that incorporate lessons learned and enhance efficiency
Serves as a common foundation and knowledge repository for GDIT and subcontractor use	A common baseline for knowledge sharing and employee and subcontractor training
Allows tailoring of standards and tools to the requirements of MA NG9-1-1	Relevant, efficient technical activities
Provides a framework for maintaining and continuously improving the standards and project management tools	Quality Assurance (QA) in all areas
Integrates tools (management, program, and technical) with the standards for monitoring and reporting	Effective management of complex, multidisciplinary projects

GDIT has developed a detailed Integrated Master Schedule (IMS) for the MA NG9-1-1 project to meet all project milestones, to include:

- System Design and Test Plan Development
- Laboratory Trial and Testing
- Data Center Installations and PSAP Pilot Deployment
- Phased PSAP Deployments
- Training
- Warranty and Maintenance

All tasks are inter-linked with accurate durations to provide status tracking, critical path, and identification of risks and issues. In concert with the IMS, a Work Breakdown Structure (WBS) has been developed and will be used for staffing requirements throughout the life cycle of the program. Milestones are linked to their actual summary-level tasks and will provide an up-to-the-minute high-level view. GDIT will use the IMS to continually assess and monitor performance, cost, and risk throughout the effort.

Figure 68 is a high-level overview of our project schedule; the detailed IMS is included in Appendix L. In addition, our detailed approach to execute to this plan is included in Section 8.13, Migration, Deployment, and Installation.

		Task Name	Duration	Start	Finish
0		Massachusetts Next-Generation 9-1-1 & ESInet System	487 days	Mon 8/4/14	Sun 5/29/16
1		Contract Award	0 days	Mon 8/4/14	Mon 8/4/14
2		Project Management	5 days	Mon 8/4/14	Fri 8/8/14
3		GDIT Procedures - Contracts/Finance/Procurement - Business Administration	5 days	Mon 8/4/14	Fri 8/8/14
4	L1	System Design & Test Plan Development (Stage 1)	417 days	Mon 8/4/14	Sun 5/1/16
5	L1.1	System Design	35 days	Mon 8/4/14	Mon 9/22/14
97	L1.2	Test Plan Development	35 days	Mon 8/4/14	Mon 9/22/14
85	8.3.4	GDIT Network Provider Agreements	35 days	Mon 8/4/14	Mon 9/22/14
99		Integrated Schedule Development	6 days	Mon 8/4/14	Mon 8/11/14
100		Kick Off Meeting	4 days	Tue 8/12/14	Fri 8/15/14
106		Inbound Carrier Trunk Coordination TASKS (2-wk prior to cuts)	33 days	Mon 8/4/14	Thu 9/18/14
111		MA NG9 1 1/GDIT Website Development	15 days	Mon 8/11/14	Sat 8/30/14
118		MA NG9 11 Site Access List	28 days	Mon 8/11/14	Thu 9/18/14
122	8.9.2	MA/GDIT Monthly Status Meetings (MA Schedule & Location)	567 days	Mon 9/1/14	Fri 4/1/16
149	8.9.2	MA/GDIT Weekly Project Status Meetings - Reports/Updates/Tracking Log	612 days	Tue 8/12/14	Tue 4/26/16
234		GDIT Weekly Conferences	612 days	Tue 8/12/14	Tue 4/26/16
323		GDIT Laboratory Hardware/Software Testing (Gold) Environment	30 days	Mon 8/11/14	Mon 9/22/14
350		Software Management, Quarterly Updates	586 days	Sat 11/1/14	Sun 5/1/16
338		GDIT/NG9-1-1 Site Survey's	158.5 days	Fri 8/15/14	Mon 4/6/15
439		GDIT/MA NG9-1-1 Initial Logistics & Procurement	34 days	Mon 8/4/14	Fri 9/19/14
459		System Design & Test Plan Development Completed	0 days	Mon 9/22/14	Mon 9/22/14
440	M1	Complete Milestone 1 (Stage 1 Deadline 3 Oct 2014)	0 days	Mon 9/22/14	Mon 9/22/14
441	L2	Laboratory Trial & Testing (Stage-2)	72 days	Mon 8/4/14	Sun 11/16/14
442	L2.1	Laboratory Trial and Testing Setup	45.25 days	Mon 8/4/14	Tue 10/7/14
455	L2.3	Change Management Protocol Development	22 days	Mon 8/4/14	Wed 9/3/14
459	L2.4	Finalize Network Design and Deployment Plans	37 days	Tue 9/23/14	Sun 11/16/14
468	L2.5	Training Plan Development	65 days	Sat 8/9/14	Wed 11/12/14
481	L2.6	Pilot Deployment Documentation and Processes	62 days	Sat 8/9/14	Thu 11/6/14
500		Data Centers Staging (2)	27.25 days	Mon 9/15/14	Thu 10/23/14
501		Equipment ship to Lab	4 days	Mon 9/15/14	Thu 9/18/14
503		Inventory & Update Database to Needham Lab Location	1 day	Fri 9/19/14	Fri 9/19/14
506		Data center 1 Equipment Staging & Core Services (T 1-2)	22.25 days	Mon 9/22/14	Thu 10/23/14
528		Data center 1 Lab Testing Complete	0 days	Thu 10/23/14	Thu 10/23/14
529		Data Center 2 Equipment Staging & Core Services (T 3-4)	22.25 days	Mon 9/22/14	Thu 10/23/14
534		Data center-2 Lab Testing Complete	0 days	Thu 10/23/14	Thu 10/23/14
555		Training Centers Staging (4)	9.75 days	Tue 10/7/14	Tue 10/21/14
556		Maynard TC CS1000 Active Backup Installation (T-1)	9.75 days	Tue 10/7/14	Tue 10/21/14
581		Maynard TC CS1000 Active Backup Lab Installation Complete	0 days	Tue 10/21/14	Tue 10/21/14
582		Maynard TC Pallas Active Backup Installation (T-2)	9.75 days	Tue 10/7/14	Tue 10/21/14
607		Maynard TC Pallas Active Backup Installation Complete	0 days	Tue 10/21/14	Tue 10/21/14
608		Taunton Training Center Active Backup Installation (T-3)	9.75 days	Tue 10/7/14	Tue 10/21/14
633		Taunton Training Center Active Backup Installation Complete	0 days	Tue 10/21/14	Tue 10/21/14
634		Springfield Training Center Installation (T-4)	9.75 days	Tue 10/7/14	Tue 10/21/14
659		Springfield Training Center Installation Complete	0 days	Tue 10/21/14	Tue 10/21/14
660		Pilot PSAPs Staging (6)	20.5 days	Thu 10/16/14	Sun 11/16/14
661		Site-1, Lab Testing, PSAP (T-1)	9.25 days	Thu 10/16/14	Wed 10/29/14
686		Site-1 Lab Testing Complete	0 days	Wed 10/29/14	Wed 10/29/14

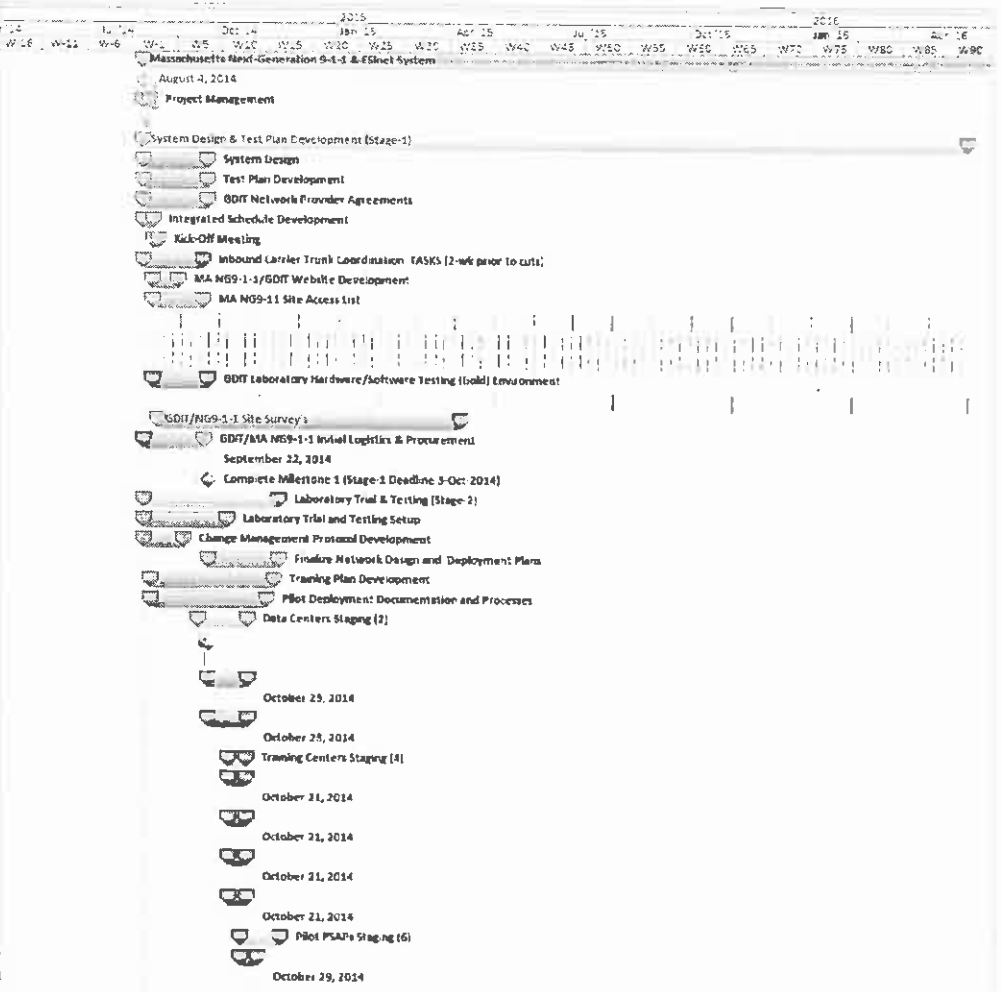


Figure 68. Integrated Master Schedule (IMS) – High-Level Overview

687		Site-2, Lab Testing, PSAP (T-2)	8.5 days	Thu 10/16/14	Tue 10/28/14
712		Site-2 Lab Testing Complete	0 days	Tue 10/28/14	Tue 10/28/14
713		Site-3, Lab Testing, PSAP (T-3)	8.5 days	Thu 10/16/14	Tue 10/28/14
738		Site-3 Lab Testing Complete	0 days	Tue 10/28/14	Tue 10/28/14
739		Site-4, Lab Testing, PSAP (T-4)	9.25 days	Thu 10/16/14	Wed 10/29/14
764		Site-4 Lab Testing Complete	0 days	Wed 10/29/14	Wed 10/29/14
765		Site-5, Lab Testing, PSAP (T-1)	11.25 days	Fri 10/24/14	Mon 11/10/14
790		Site-5 Lab Testing Complete	0 days	Mon 11/10/14	Mon 11/10/14
791		Site-6, Lab Testing, PSAP (T-2)	9.25 days	Wed 10/22/14	Tue 11/4/14
816		Site-6 Lab Testing Complete	0 days	Tue 11/4/14	Tue 11/4/14
817		Laboratory Trial & Testing Complete	0 days	Sun 11/16/14	Sun 11/16/14
818	M2	Complete Milestone 2 (Stage 3 Deadline 9-Dec-2014)	0 days	Sun 11/16/14	Sun 11/16/14
819	L3	Data Center, Training Centers & Pilot PSAPs Deployment (Stage 3)	57 days	Mon 11/17/14	Mon 2/9/15
820	L3.1	Data Center Installations	14 days	Mon 11/17/14	Fri 12/5/14
825	L3.2	Training Center Installation	7 days	Thu 1/29/15	Fri 2/6/15
827	L3.3	PSAP Pilot Deployment	50 days	Wed 11/26/14	Mon 2/9/15
830		Data Center Deployments	55.5 days	Mon 11/17/14	Fri 2/6/15
831	L3.1	Data center-1 Deployment (Teams 1-2)	55.5 days	Mon 11/17/14	Fri 2/6/15
892		Data Center 1 Deployment Completed	0 days	Thu 1/22/15	Thu 1/22/15
893	L3.1	Data center-2 Deployment (Teams 3-4)	55.5 days	Mon 11/17/14	Fri 2/6/15
954		Data Center-2 Deployment Completed	0 days	Thu 1/22/15	Thu 1/22/15
955		Training Centers Deployment	55.5 days	Fri 11/21/14	Thu 2/12/15
956		Maynard TC C51000 Active Backup Deployment (T-1)	55.5 days	Fri 11/21/14	Thu 2/12/15
1011		Maynard TC C51000 Active Backup Deployment Complete	0 days	Wed 1/28/15	Wed 1/28/15
1012		Maynard TC Pallas Active Backup Deployment (T-2)	55.5 days	Fri 11/21/14	Thu 2/12/15
1069		Maynard TC Pallas Active Backup Deployment Complete	0 days	Wed 1/28/15	Wed 1/28/15
1070		Taunton Training Center Active Backup Deployment (T-3)	55.5 days	Fri 11/21/14	Thu 2/12/15
1126		Taunton Training Center Active Backup Deployment Complete	0 days	Wed 1/28/15	Wed 1/28/15
1127		Springfield Training Center Deployment (T-4)	55.5 days	Fri 11/21/14	Thu 2/12/15
1183		Springfield Training Center Deployment Complete	0 days	Wed 1/28/15	Wed 1/28/15
1184		Pilot PSAP Deployment	60.5 days	Wed 11/26/14	Wed 2/25/15
1185	& 11.7	Submit Final Disaster Recovery/Business Continuity Plan (Only 1st Pilot PSAP)	0 days	Wed 11/26/14	Wed 11/26/14
1186		Pilot 1 PSAP Deployment (T-1)	55.5 days	Fri 11/28/14	Thu 2/19/15
1242		PSAP 1 Staging & Deployment Completed	0 days	Wed 12/17/14	Wed 12/17/14
1243		Pilot 2 PSAP Deployment (T-2)	55.5 days	Fri 11/28/14	Thu 2/19/15
1299		PSAP 2 Staging & Deployment Completed	0 days	Wed 12/17/14	Wed 12/17/14
1300		Pilot-3 PSAP Deployment (T-3)	55.5 days	Fri 11/28/14	Thu 2/19/15
1356		PSAP 3 Staging & Deployment Completed	0 days	Wed 12/17/14	Wed 12/17/14
1357		Pilot-4 PSAP Deployment (T-4)	55.5 days	Fri 11/28/14	Thu 2/19/15
1413		PSAP 4 Staging & Deployment Completed	0 days	Wed 12/17/14	Wed 12/17/14
1414		Pilot-5 PSAP Deployment (T-1)	55.5 days	Thu 12/4/14	Wed 2/25/15
1470		PSAP 5 Staging & Deployment Completed	0 days	Tue 12/23/14	Tue 12/23/14
1471		Pilot-6 PSAP Deployment (T-2)	55.5 days	Thu 12/4/14	Wed 2/25/15
1527		PSAP 6 Staging & Deployment Completed	0 days	Tue 12/23/14	Tue 12/23/14
1528		Mobile PSAP, Schedule , Teams 3-4	8 days	Wed 12/17/14	Tue 12/30/14
1544		Mobile PSAP Installation Completed	0 days	Tue 12/30/14	Tue 12/30/14
1545		Data Center, Training Centers & Pilot PSAP Deployment Completed	0 days	Mon 2/9/15	Mon 2/9/15

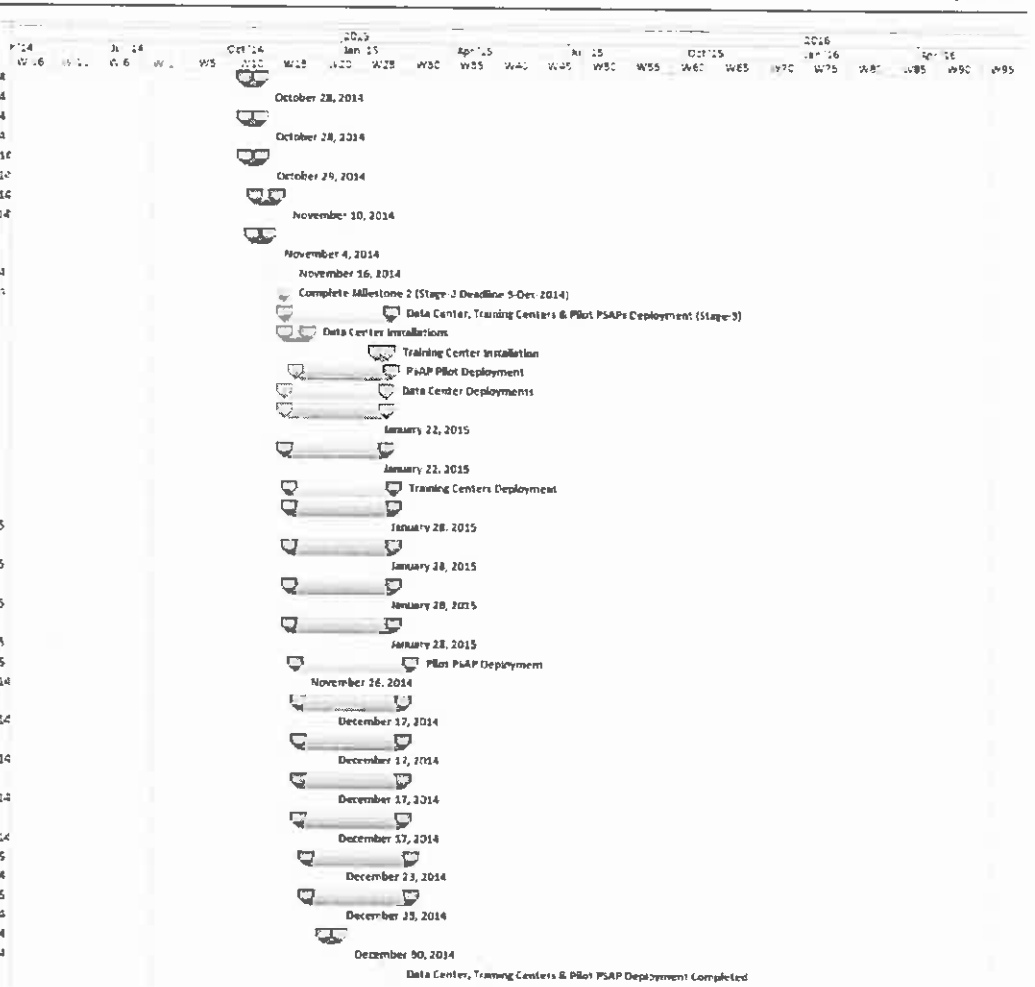


Figure 68. Integrated Master Schedule (IMS) – High-Level Overview (Cont.)

ID	RFP#	Task Name	Duration	Start	Finish
1548	M3	Complete Milestone 3 (Stage 4 Deadline 27 Feb 2015)	0 days	Mon 2/9/15	Mon 2/9/15
1549	L4	PSAP Deployment (Stage-4)	498.5 days	Sat 1/10/15	Sun 5/29/16
1549	L4.1	Group 1 Deployments (20)	83 days	Sat 1/10/15	Sat 5/9/15
1549		PSAP Deployment	0 days	Mon 2/9/15	Mon 2/9/15
1550		Team 1	83 days	Sat 1/10/15	Sat 5/9/15
1551	L4.1.1	PSAP 1 Deployment	65.5 days	Sat 1/10/15	Wed 4/15/15
1612	L4.1.2	PSAP 2 Deployment	67.5 days	Wed 1/14/15	Tue 4/21/15
1743	L4.1.3	PSAP 3 Deployment	67.5 days	Wed 1/21/15	Mon 4/27/15
1798	L4.1.4	PSAP 4 Deployment	68 days	Tue 1/27/15	Sun 5/3/15
1875	L4.1.5	PSAP 5 Deployment	69 days	Mon 2/2/15	Sat 5/9/15
1956		Team 2	83 days	Sat 1/10/15	Sat 5/9/15
1957	L4.1.6	PSAP 6 Deployment	65.5 days	Sat 1/10/15	Wed 4/15/15
2038	L4.1.7	PSAP 7 Deployment	67.5 days	Wed 1/14/15	Tue 4/21/15
2119	L4.1.8	PSAP 8 Deployment	67.5 days	Wed 1/21/15	Mon 4/27/15
2200	L4.1.9	PSAP 9 Deployment	68 days	Tue 1/27/15	Sun 5/3/15
2281	L4.1.10	PSAP 10 Deployment	69 days	Mon 2/2/15	Sat 5/9/15
2362		Team 3	83 days	Sat 1/10/15	Sat 5/9/15
2363	L4.1.11	PSAP 11 Deployment	65.5 days	Sat 1/10/15	Wed 4/15/15
2444	L4.1.12	PSAP 12 Deployment	67.5 days	Wed 1/14/15	Tue 4/21/15
2525	L4.1.13	PSAP 13 Deployment	67.5 days	Wed 1/21/15	Mon 4/27/15
2606	L4.1.14	PSAP 14 Deployment	68 days	Tue 1/27/15	Sun 5/3/15
2687	L4.1.15	PSAP 15 Deployment	69 days	Mon 2/2/15	Sat 5/9/15
2768		Team 4	83 days	Sat 1/10/15	Sat 5/9/15
2769	L4.1.16	PSAP 16 Deployment	65.5 days	Sat 1/10/15	Wed 4/15/15
2850	L4.1.17	PSAP 17 Deployment	67.5 days	Wed 1/14/15	Tue 4/21/15
2931	L4.1.18	PSAP 18 Deployment	67.5 days	Wed 1/21/15	Mon 4/27/15
3012	L4.1.19	PSAP 19 Deployment	68 days	Tue 1/27/15	Sun 5/3/15
3093	L4.1.20	PSAP 20 Deployment	69 days	Mon 2/2/15	Sat 5/9/15
3174		Group-1 Cutover Acceptance Reports Approved	0 days	Fri 4/24/15	Fri 4/24/15
3175		Complete Stage-4 Group 1 Milestone (April 30, 2015)	0 days	Fri 4/24/15	Fri 4/24/15
3176	L4.2	Group-2 Deployments (30) Framingham	66 days	Wed 3/11/15	Thu 6/11/15
3180	L4.3	Group-3 Deployments (34)	68 days	Thu 4/30/15	Mon 8/3/15
3188	L4.4	Group 4 Deployments (34) Worcester	70 days	Mon 6/22/15	Tue 9/29/15
3188	L4.5	Group-5 Deployments (28)	58 days	Tue 8/18/15	Mon 11/9/15
3192	L4.6	Group 6 Deployments (35) Springfield	73 days	Mon 9/28/15	Wed 1/13/16
3196	L4.7	Group-7 Deployments (35) Boston	77 days	Tue 12/1/15	Tue 3/22/16
3200	L4.8	Group-8 Deployments (35)	78 days	Tue 2/9/16	Sun 5/29/16
3201		PSAP Sites 216 thru 248	12 days	Tue 2/9/16	Thu 3/24/16
3202	L4.8.249	PSAP 249 Deployment (Team 2)	68 days	Wed 2/24/16	Sun 5/29/16
3283	L4.8.250	PSAP 250 Deployment (Team 3)	68 days	Wed 2/24/16	Sun 5/29/16
3364	L4.8.251	PSAP 251 Deployment (Team-4)	68 days	Wed 2/24/16	Sun 5/29/16
3445		Group-8 Cutover Acceptance Reports Approved	0 days	Fri 4/29/16	Fri 4/29/16
3446		Complete Stage-4 Group 8 Milestone (June 30, 2016)	0 days	Fri 4/29/16	Fri 4/29/16
3447	M4	Complete Milestone 4 (Stage-4 Deadline 30 Jun 2016)	0 days	Fri 4/29/16	Fri 4/29/16
3448		Maintenance/Sustainment - Start, Post Milestone-4 Completion	0 days	Fri 4/29/16	Fri 4/29/16
3449		GDIT/Windstream NOC/SOC, Depot/Spares, Training	0 days	Fri 4/29/16	Fri 4/29/16

Figure 68. Integrated Master Schedule (IMS) – High-Level Overview (ConL)

Management Approach

GDIT's project management approach is built around four tenets that together will provide the Commonwealth the lowest risk for a successful project outcome. These tenets are:

- **Maintain Continuity with Least Risk** – We assign experienced personnel who have the demonstrated applicable experience, capabilities, established customer relationships, and historical knowledge. Maintaining personnel continuity provides the lowest performance risk while advancing to successfully completing the project.
- **Shared Governance** – Our team adheres to the overarching principle of joint guidance across the customer and GDIT partnership. We will help manage, consult, coach, mentor, and facilitate stakeholder collaboration throughout the duration of the project.
- **Right Mix of Capabilities and Skills** – Our management and engineering teams have the right mix of capabilities covering the depth and range of skills required to overcome complex technical challenges and minimizes performance delays.
- **Advance Technologies and Processes** – Leverage GDIT and partner research and design activities to enhance the environment.

Subcontractor Approach

GDIT understands the risks associated with teaming with other subcontractors in the performance of a large-scale project. GDIT minimizes this risk by pre-qualifying subcontractors for specific work scope areas. GDIT instituted a program called the Quality Service Provider (QSP) whereby subcontractors have been prequalified and are available to perform work immediately. This program has been administered as part of our Quality, Environmental, Health, and Safety (QEHS) program since the early 2000's. GDIT has successfully implemented this methodology for over seventeen years, and has over 100 subcontractors prequalified and ready to perform a wide array of support functions as needed. For this project, we have pre-qualified Massachusetts-based and certified Minority and Women-Owned Businesses and Service-Disabled Veteran-Owned Business Enterprises (SDVOBE) to support the installation and maintenance phases.

Managing the Build-Out and Integration

GDIT manages large-scale efforts using an Integrated Master Schedule (IMS) and Contractor Work Breakdown Structure (CWBS) to continually assess and monitor performance, cost, and risk throughout the effort. The integration will also be managed through routine meetings and discussions between GDIT's program support, technical leads, and Commonwealth counterparts to review planned scheduled events, required resources, and activity coordination between the identified tasks. GDIT understands that communication, collaboration, and coordination are essential in this dynamic environment. Our strategy is to work closely with the customer under a transparent governance organizational structure that facilitates communication, collaboration, and teamwork towards shared goals and objectives. We routinely engage our customer leads on all technical and management aspects of the program. GDIT supports a complete portfolio of program status reporting that include: (1) weekly business meetings to review all contract related items, (2) weekly "Newsflash " meetings to review program status, and (3) weekly "Dashboard"

meetings that are specific to each/any phase under the program. In addition, GDIT performs monthly status meetings that review the total project.

Meeting discussions include assessing performance against the IMS, capturing updates based on priority changes, and fully vetting and coordinating between the functions. GDIT continuously addresses cost and assesses risks for all schedule updates. Costs will be assessed against the CWBS and performance metrics with recommended adjustments to resource allocations aligned to an updated IMS. Risks will be assessed to identify issues and or conflicts between the functions.

Risk Management

GDIT's risk mitigation process is based on the principle that risk management must be forward-looking, structured, collaborative, continuous, and an integral part of the overall decision-making process. At the outset of the program, we will establish a risk management plan that provides a structured method to identify, analyze, plan, monitor, control, and communicate potential program risks. We will establish an internal Risk Management Board (RMB) that tracks risks internally on the GDIT's Risk Register. Risks are typically identified through daily collaboration between program engineering staff, GDIT's Task Leads, Commonwealth counterparts, and stakeholders when discussing planned phase implementation activities. From these discussions we identify risks, impacts, and mitigation options. We document these risks into the Risk Register and conduct a weekly internal RMB meeting led by the Program Manager, engineering staff, and Technical Leads, to coordinate actions required.

In addition to the Risk Management Plan, an Issue Management Plan will be developed to handle project issues that have occurred and that need to be addressed in an immediate fashion, This process will bring visibility to issues, accountability to how they are acted upon, and their timely resolution. Related discussions and associated actions will be logged.

Project Management Tools

Upon award, GDIT's Project Team will meet with the Commonwealth to begin the Initiation and Planning phases of the project. During these sessions, sponsors and stakeholders will be confirmed, the charter will be finalized, objectives and goals will be identified and formalized, and critical success factors will be documented. Methodologies of tracking scope, cost, labor, risk, and change will reviewed and agreed to. A Communication Plan will be reviewed and implemented to include tools that will be used for tracking the project. Dates and times of weekly project calls will be established as well as reoccurring project reporting to include weekly reports, action items, risk tracking, budget tracking, meeting minutes, and monthly report deliveries. Acceptance criteria will be formalized through the Transition Plan. The Issues Management and Escalation Plan will also be reviewed. Agreement will be made on the Contract Administration Plan and how we will conduct business.

The Project Plan as well as the Statement of Work will be reviewed and finalized following technical discussion and agreement on the scope of the project. Methodology for change management will be finalized to include how change is identified, who is notified, who is responsible for identifying financial impact and risk analysis of the change, and who is authorized to sanction the change as well as how it is formally implemented.

A Responsibility Assignment Matrix will also be finalized and approved at this time identifying both GDIT and Commonwealth tasks and responsible parties.

A review of the Schedule Management Guidelines and the current schedule will be conducted. We will discuss our resource plan and methodology as well as how we will manage our subcontractors.

Risk and risk mitigation will be discussed, and risk will be continuously tracked during the duration of the project. The Risk Management Plan will describe how we will identify, value, mitigate, report, and track risks as well as project budget impacts.

Finally, GDIT's Quality Management Plan will be presented, demonstrating to the Commonwealth our commitment to ensure our proven quality processes are incorporated in our execution of this program.

Following finalization of the Management Plans, GDIT will review with the Commonwealth current project status, identified risks, and scope changes as well as any additional goals and objectives The purpose of this review is to get approval from the stakeholders to proceed to the Executing phase.

During the Executing phase, GDIT will implement the project according to the established schedule and Management Plans. We will follow the procedures outlined in the plans for tracking, reporting, updating, mitigating, and completing the tasks identified in the project schedule. As tasks are completed, we will seek formal acceptance from the sponsors identified in the Transition Plan.

At the time of system acceptance, GDIT will support the Closure stage of the project by ensuring that the project has been successfully handed off to the end users and GDIT's support team. All required project documentation including as-built documentation will be completed and submitted. GDIT will support the development of the post-implementation project report and lessons learned as necessary.

All written documents will be delivered in machine-readable format, capable of being completely and accurately reproduced by computer software on a laser printer. All itemized and/or annotated lists will be delivered in computer spreadsheets, capable of being imported to Microsoft Excel 2007 or higher. All meetings will be held at the offices of the State 911 Department, unless agreed to otherwise by the State 911 Department.

GDIT represents and warrants to the State 911 Department that we will be sufficiently staffed and equipped to fulfill GDIT's obligations under the contract, GDIT's services will be performed by appropriately qualified and trained personnel, with due care and diligence and to a high standard of quality as is customary in the industry, in accordance with the terms and conditions of the contract and in accordance with all applicable professional standards.

GDIT will ensure that appropriate organizational management has authority to exercise decision-making over contractual matters, and that GDIT will escalate such matters to the appropriate organizational level.

The Project Organization Structure and staffing plan is provided in Section 9, Bidder Qualifications.

8.9.1. Contract Manager

The contractor shall designate a Contract Manager assigned to meet the State 911 Department's needs under the contract and any renewals thereof. The Contract Manager shall be responsible for oversight and management of contract performance and shall act as the primary contact person for receipt of notice and other communications under the contract, including but not limited to, timely reports and written responses and attendance at meetings as required by the State 911 Department. The Contract Manager shall not be changed without the prior written approval of the State 911 Department.

GDIT selected Mr. Stephen Woodworth to be our Contract Manager to meet the State 911 Department's needs under the contract and any renewals thereof. Mr. Woodworth has more than twenty years' experience managing, negotiating, and drafting complex contractual arrangements for commercial and government customers. Mr. Woodworth brings direct experience working on key statewide public safety projects such as the State of New York Statewide Wireless Radio Network, where he served as GDIT's Contracts Manager.

Mr. Woodworth will be responsible for oversight and management of contract performance and will act as the primary contact person for receipt of notice and other communications under the contract, including but not limited to, timely reports and written responses and attendance at meetings as required by the State 911 Department. GDIT agrees that the Contract Manager will not be changed without the prior written approval of the State 911 Department.

Mr. Woodworth's resume is included in Section 9 (Bidder Qualifications) of this proposal.

8.9.2. Project Manager

As noted above, the contractor shall, at a minimum, designate a project manager, and the designated project manager shall perform project management on behalf of the contractor. The project manager shall be a certified project management professional and shall have obtained the PMI Project Management Professional, or PMP, designation. The Project Manager shall not be changed without the prior written approval of the State 911 Department.

The project manager shall:

- *Be responsible for administering the agreement and the managing of the day-to-day operations of the project;*
- *Serve as an interface between the State 911 Department and all contractor personnel participating in the project;*
- *Develop and maintain the Project Management Plan, in consultation with the State 911 Department;*
- *Be located in Commonwealth and shall be available to be on-site at the State 911 Department's offices within two (2) hours of receipt of a request from the State 911 Department;*
- *Facilitate regular communication with the State 911 Department, including weekly status reports/updates, and review the project performance against the project plan. Facilitate weekly project status meetings for the duration of the engagement;*
- *Provide all documentation to be discussed at scheduled meeting at least twenty-four (24) hours prior to said scheduled meeting;*
- *Update the project plan on a weekly basis and distribute at weekly meetings for the duration of the engagement;*
- *Sign acceptance forms to acknowledge their receipt from State 911 Department;*
- *Be responsible for the management and deployment of contractor personnel;*
- *Participate in regular meetings, at least monthly, or as otherwise scheduled by State 911 Department personnel, to take place on-site at the offices of the State 911 Department or via telephone conference call;*
- *Coordinate with any and all subcontractors to ensure that any and all subcontractors participate at meetings or on conference calls;*
- *Adhere to change management protocols;*

- *Participate and assist on special projects at the request of the State 911 Department with pricing to be negotiated as assigned; and*
- *Provide a customer informational bridge, within fifteen (15) minutes of a request by the State 911 Department, for the purposes of information sharing, data gathering, and coordination.*

GDIT selected Mr. Paul Chotkowski as our designated overall Project Manager. Mr. Chotkowski has extensive experience managing large complex multi-faceted projects including public safety projects to include a multi-site U.S. Air Force First Responder deployment of 100 PSAP workstations across 48 U.S. Air Force bases worldwide. Mr. Chotkowski has over 15 years of project management experience.

A member in good standing of the Project Management Institute, he obtained his Project Management Professional (PMP) designation in 2001, possessing PMP certificate number 34874. His current certification is valid through 27 June 2017. GDIT agrees that the Project Manager will not be changed without the prior written approval of the State 911 Department.

Utilizing our established program management tools and processes, Mr. Chotkowski will:

- Be responsible for administering the agreement and managing the day-to-day operations of the project.
- Serve as the interface between the State 911 Department and all contractor personnel participating in the project.
- Develop and maintain the Project Management Plan in consultation with the State 911 Department.
  - The Project Management Plan governs our management, engineering, development, help desk, logistics, and administrative personnel to effectively provide services for the MA NG9-1-1 project.
  - The Project Management Plan provides our team a single comprehensive approach to meeting all program requirements.
  - Mr. Chotkowski will provide the Project Management Plan to the Commonwealth for review and approval to ensure we operate under a common framework towards achieving performance, cost, and schedule objectives
- Mr. Chotkowski resides in Mansfield, Massachusetts and can be on-site at the State 911 Department's offices within two (2) hours of receipt of a request from the State 911 Department.
- Facilitate regular communication with the State 911 Department, including weekly status reports/updates, and review the project performance against the project plan. Facilitate weekly project status meetings for the duration of the engagement. An action register and meeting minutes will be maintained and distributed according to the Communications Plan.
- Provide all documentation to be discussed at scheduled meeting at least twenty-four (24) hours prior to said scheduled meeting;

- Update the project plan on a weekly basis and distribute at weekly meetings for the duration of the engagement;
- Sign acceptance forms to acknowledge their receipt from State 911 Department;
- Be responsible for the management and deployment of contractor personnel;
- Participate in regular meetings, at least monthly, or as otherwise scheduled by State 911 Department personnel, to take place on-site at the offices of the State 911 Department or via telephone conference call. Typical items to be discussed at scheduled meetings include the following; however, specific items will be identified within the Communication Plan developed for the project:
  - Activity summary
  - Major milestones
  - Open action items
  - Program risks and response to risks
  - Modification progress to schedule performance
  - Major activities planned for the succeeding month
  - Status of baseline changes
- GDIT has a large meeting facility in our Taunton facility that can accommodate large groups, and it will be made available as needed to the Massachusetts NG9-1-1 project members;
- Coordinate with any and all subcontractors to ensure that any and all subcontractors participate at meetings or on conference calls;
- Adhere to change management protocols;
- Participate and assist on special projects at the request of the State 911 Department with pricing to be negotiated as assigned; and
- Provide a customer informational bridge, within fifteen (15) minutes of a request by the State 911 Department, for the purposes of information sharing, data gathering, and coordination.

Mr. Chotkowski's resume is included in Section 9 (Bidder Qualifications) of this proposal.

8.9.3. Change Management

Bidders shall employ change management protocols and shall describe in detail their procedures for service and change management processes that shall include all aspects of the project, including without limitation, data center, network, and CPE build documents. The contractor shall use best practices using the ITIL framework to improve service, manage change, and minimize downtime. The contractor shall provide change management reports for system and other changes.

GDIT has a staff of more than 1,000 Information Technology Infrastructure Library (ITIL) certified employees who apply the best practices of ITIL to deliver superior results. As a large systems integrator, we support ITIL practices in the three primary areas of Service Design, Service Transition, and Service Operation across our project base, so that employees understand how to build, transition, and operate effective overall systems. We ensure that processes are in

place and are properly followed to improve service, manage change, and minimize downtime. Knowledge and experience in these primary areas enable our team to understand the ramifications of the decisions made during each phase, and to consider each decision to provide the best overall value and service delivery for the Commonwealth. For the Commonwealth NG9-1-1 project, we will pay particular attention to the application of ITIL best practices for data center, network, and CPE build documents.

GDIT has in place a robust change management process. A change, including a change register report, for the MA NG9-1-1 project will be developed during the planning phase of the project and presented for approval by the MA NG9-1-1 project office. Under the direction of the Project Manager, GDIT's Configuration Manager will oversee the Configuration Management (CM) process and use the GDIT Configuration Management System (CMS) to manage and control engineering records and data. The CMS is an integrated CM system consisting of policies, processes, procedures and an automated tool set for information management. Under the direction of the Project Manager, the Configuration Manager coordinates the approval and release of deliverable technical documentation, CM interfaces, the establishment of program CM baselines, the review and approval of deliverable document changes, configuration audits (coordinated with the Quality Assurance (QA) Manager), the configuration verification of assets and program developed products, and the processing of all deliverable technical documents until contract closure.

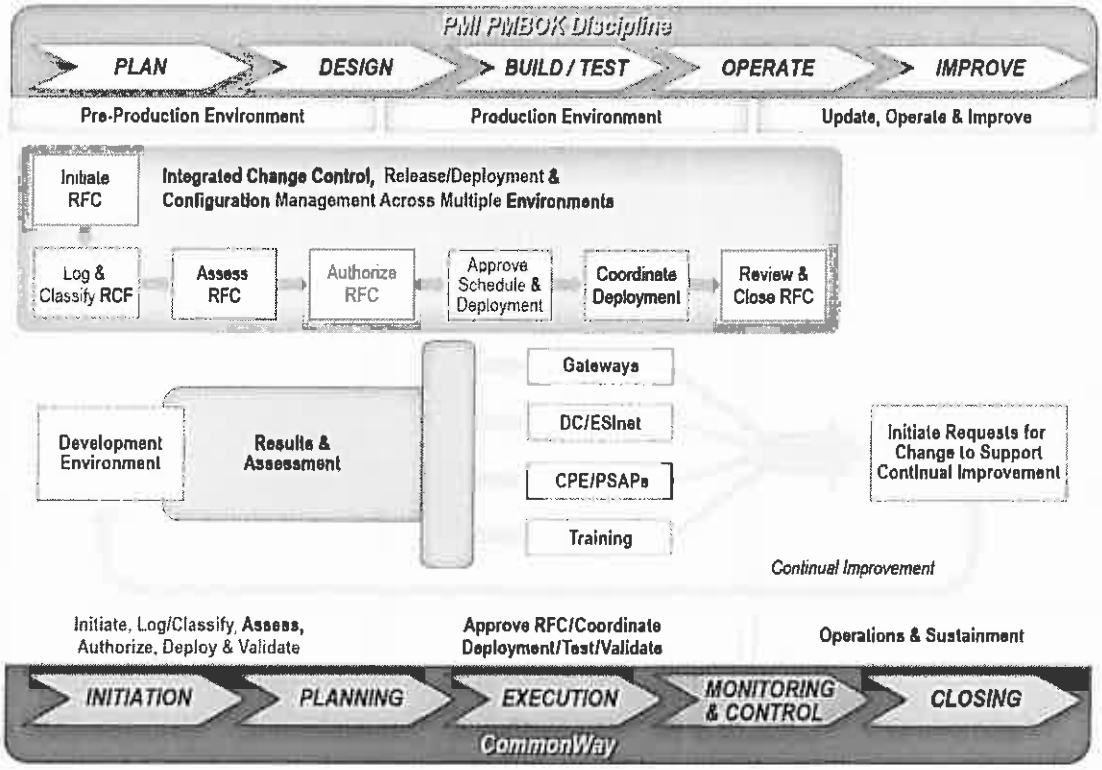


Figure 69. Configuration Management System (CMS)

The Configuration Manager has overall responsibility for ensuring that all documents, including forms used to create quality records, are controlled as summarized below:

- Approve documents for adequacy prior to issue.
- Review, update as necessary, and re-approve documents.
- Identify the current revision status of documents.
- Ensure that relevant versions of applicable documents are available at points of use.
- Ensure that documents remain legible, readily identifiable, and retrievable.
- Ensure that documents of external origin (including customer engineering standards and specifications) are identified and their distribution controlled.
- Prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose. GDIT will be guiding the CM effort for the consortium, laying the framework for the team that will be utilized for all project-related CM processes.

8.10. SYSTEM RELIABILITY AND AVAILABILITY REQUIREMENTS

The system, including all subsystems, shall be available a minimum of 99.999% of the time when measured on a 24 x 7 basis during a calendar year, including system maintenance and upgrades. Availability may be achieved through redundancy or fault tolerance. Bidders shall demonstrate how the system shall achieve this requirement.

The system shall be sized to handle the current and anticipated volume of transactions and activities and the projected anticipated volume of transactions and activities. The historical call volume data is set forth on Attachment K2– Primary PSAP, Regional PSAP, and RECC Data.

The estimated elapsed time for call delivery shall not exceed one (1) second, measured from the time the call is presented to the ESInet until the call is delivered to the PSAP. For each call type, the contractor shall measure the elapsed time for call delivery to the appropriate PSAP and shall provide test results.

GDIT will comply with the RFR specifications.

System reliability and availability are critical considerations that are within GDIT's proposed solution architecture. GDIT's solution design is also sized to handle all 9-1-1 calls and payloads regardless of independent equipment failure, data center failure, ESInet failure, PSAP failure, or WAN failure. Redundancy and diversity are key elements contained in GDIT's solution.

The following descriptions demonstrate how the system will achieve a minimum of 99.999% availability including during system maintenance and upgrade windows.

As discussed previously, GDIT's solution is comprised of two (2) geographically diverse high-availability data center facilities that include a variety of environment redundancies including power, HVAC, and diverse carrier entries as well as carrier diverse 10 GB capable links between the two data centers (see Section 8.5. Data Centers for detailed information). During transition and until the ILEC's selective routers are decommissioned, circuits from the selective routers and carriers will be dual-homed to each of the data centers to ensure that even if a data center were to become completely unavailable, all 9-1-1 calls will still be delivered to the PSAPs. Contained within each of the data centers are highly redundant ESInets that are interconnected via diverse 1GB point-to-point private circuits.

Each ESInet is designed to handle 100% of the Commonwealth's 9-1-1 payload traffic. Each element within the ESInet is configured for redundancy, so if any one ESInet element or combination of ESInet elements fail, the entire system and call loads remain operational. Network elements (routers/switches), servers, and storage are all designed for fault tolerance via clustering, virtual servers, RAID striping, and a redundant routing and switching fabric for transport.

PSAPs are also designed for high availability. As designated by the State 911 Department, redundant circuits, routers, and switches are used to ensure the highest level of availability is achieved at the designated PSAPs. However, even if a PSAP were to become unavailable, GDIT's solution takes that into consideration to ensure the availability requirements are met.

The IP ACD call taking CPE system within the ESInet is a critical element contained within each ESInet to ensure availability requirements are met.

GDIT is proposing ECW's CallStation for the IP ACD call taking CPE solution – specifically for its fault tolerant high-availability capabilities. The proposed CPE solution provides non-blocking, fault-tolerant switching with an architecture that supports active-active failover. The proposed CPE solution architecture is a CPE blade server supercluster that acts as one unified system within two or more data centers. Each cluster within the supercluster is fault tolerant even in the event of a hardware failure (e.g., a server goes down within a cluster).

Additionally, voice and data are automatically re-routed within the CPE solution should a PSAP position or entire PSAP become unavailable. Unlike other competing systems, GDIT's proposed CPE solution checks the availability of the remote PSAP *each time a call is routed* and provides instant failback when the PSAP returns to availability.

The processing and re-routing of voice and data payloads also occur in the event of ring timeout, or when the PSAP's configured maximum number of calls waiting is exceeded. The proposed CPE solution also re-routes calls if they have not been answered within a configurable amount of time and can also re-route based on a configurable number of calls that are already holding for answer.

All elements of the WAN, data centers, ESInets, and PSAPs are monitored 24x7x365 via GDIT's NSOC to ensure service affecting and non-service affecting events are responded to based on escalation procedures and response times that meet or exceed the standards set forth in 560 CMR 2.00 as well as those response times contained within Section 8.20.12, Notification and Escalation.

In addition, elapsed time for call delivery will be measured and reported per appropriate PSAP.

System Maintenance and Upgrade Windows

Availability requirements will be maintained during system maintenance and upgrades because GDIT will follow well-developed processes that align with ITIL best practices. Changes will be well documented, reviewed, and approved by the Commonwealth's designated approval authority. GDIT's redundant and highly available architecture enables the Commonwealth to realize the benefits of an IP-based NG9-1-1 solution. The IP-based network routing combined with the capabilities of the IP-based CPE enables automatic call routing to available PSAPs. Call routing can also be purposefully configured should the Commonwealth decide during the

approval process that system maintenance or an upgrade require a prescribed call routing solution. Although an unlikely scenario due to the highly redundant component architecture within each ESInet, there is an option to route all 9-1-1 traffic to one single ESInet during a maintenance window since each ESInet is designed to handle 100% of the call handling.

8.10.1. Software Upgrades and Documentation

Bidders shall describe how they propose to provide operating system and/or software upgrades without adversely impacting service availability or performance.

When software updates or enhancements become available, the contractor shall notify the State 911 Department of such availability as soon as possible following the manufacturer's release announcement. The State 911 Department shall then have the opportunity to request installation of the new software, which shall be installed by the contractor at no charge to the State 911 Department. However, when such software releases are intended by the manufacturer as generic version updates to correct reproducible and/or recurring defects (software bugs), these releases shall be installed by the contractor upon prior approval by the State 911 Department at no charge to the State 911 Department. Software updates for this system shall be supplied for the duration of the contract utilizing defined change management protocols.

The contractor shall provide the State 911 Department with a comprehensive inventory of all current release versions which shall include any operating systems and application software, in a document entitled "Software Inventory." Prior to delivery of the CPE at the PSAP, the contractor shall install the latest software versions and/or patches applied to all components of the system. These latest versions shall be mutually agreed upon by the State 911 Department and the contractor. The contractor shall provide a checklist, previously verified by the State 911 Department, to technicians performing the installations, to be used by the technicians to verify that the software versions installed are those that were mutually agreed upon by the State 911 Department and the contractor.

GDIT will comply with the RFR specification.

Our team understands the necessity of maintaining operations of critical networks and the maintenance of these systems through software updates and upgrades cannot interrupt the processing of emergency services. GDIT has established procedures for ensuring availability of systems, while at the same time ensuring applications and operating systems stay up-to-date and secure. Our process starts with identification of available (notification to be provide to the State 911 Department) updates from the various software vendors providing products the NG9-1-1 system. Our engineering staff reviews the necessity of applying available updates in the context of the system. Not all available patches and upgrades are required to be applied. If identified software updates are deemed necessary for the NG9-1-1 system, we will document the required installation procedures and develop a test plan to ensure the application of the upgrade does not adversely affect system operation.

Figure 70. Software Upgrade Process

The software update is then applied to an offline system in our development facility that is identical in hardware and software to the production system utilizing the installation instruction instructions created to verify their accuracy. The test plan is then run against the development system to ensure proper operation of the system. GDIT then meets the State 911 Department with all available information about the upgrade, including results of testing and a recommendation and installation plan for application to the production system(s). All such plans

include a rollback procedure in the event the application causes unintended consequences to the system; the installing technician can quickly and easily return the system to its prior configuration. In the MA NG9-1-1 system, we will utilize the built in redundancy of the system to minimize downtime. Where an upgrade may cause interruption to service, we will apply such updates during off-peak traffic hours. In all cases, the upgrade schedule and plan will be coordinated with the State 911 Department for approval.

As part of our software configuration management process, GDIT maintains a database of the current software and hardware baseline. This database lists all hardware platforms in the entire system with every software package installed, including operating systems and current version levels. This database will also include the development environment. For the MA NG9-1-1 system, this "Software Inventory" will be maintained by our NSOC personnel, and all changes to the baseline will be coordinated with the State 911 Department as part of the configuration management process. As new PSAP CPE equipment is deployed, the latest approved versions of hardware and software will be utilized. In all cases, technician and/or NSOC personnel performing installations and upgrades will utilize the installation procedures developed by our engineering team, validated in the development environment, and approved by the Commonwealth. Test procedures will be executed to confirm proper installation.

8.10.2. Configuration Documentation and Changes

The contractor shall provide the State 911 Department with configuration documentation in a mutually agreed upon format.

The contractor shall provide the State 911 Department with a standard change management document that will describe any software or hardware system or manufacturer default setting changes that are implemented by the contractor in the staging facility. Any change shall be approved by the State 911 Department prior to the execution of a change. The contractor shall, if the standard change management document is updated or revised, promptly provide to the State 911 Department with a new version of the change management document. The contractor shall follow industry standards best practices such as ITIL or the equivalent, and shall maintain a change management database that can be accessed by the State 911 Department.

GDIT will comply with the RFR specification.

With our extensive experience in providing and maintaining mission-critical systems for the DoD, GDIT is intimately familiar with acute technical discipline that must be exercised when deploying and managing critical information technology solutions, such as NG9-1-1. Our well-defined configuration document and the standard change management document, along with practice of technical discipline, will prevent catastrophic system failures. GDIT will develop and maintain standard change management documents and follow industry standards best practices throughout the life cycle of the MA NG9-1-1 system.

Our configuration management process will systematically ensure that the NG9-1-1 system's performance, functional, and physical attributes maintain their integrity over time. Our systematic process of developing configuration documents and the change process is depicted in Figure 71.

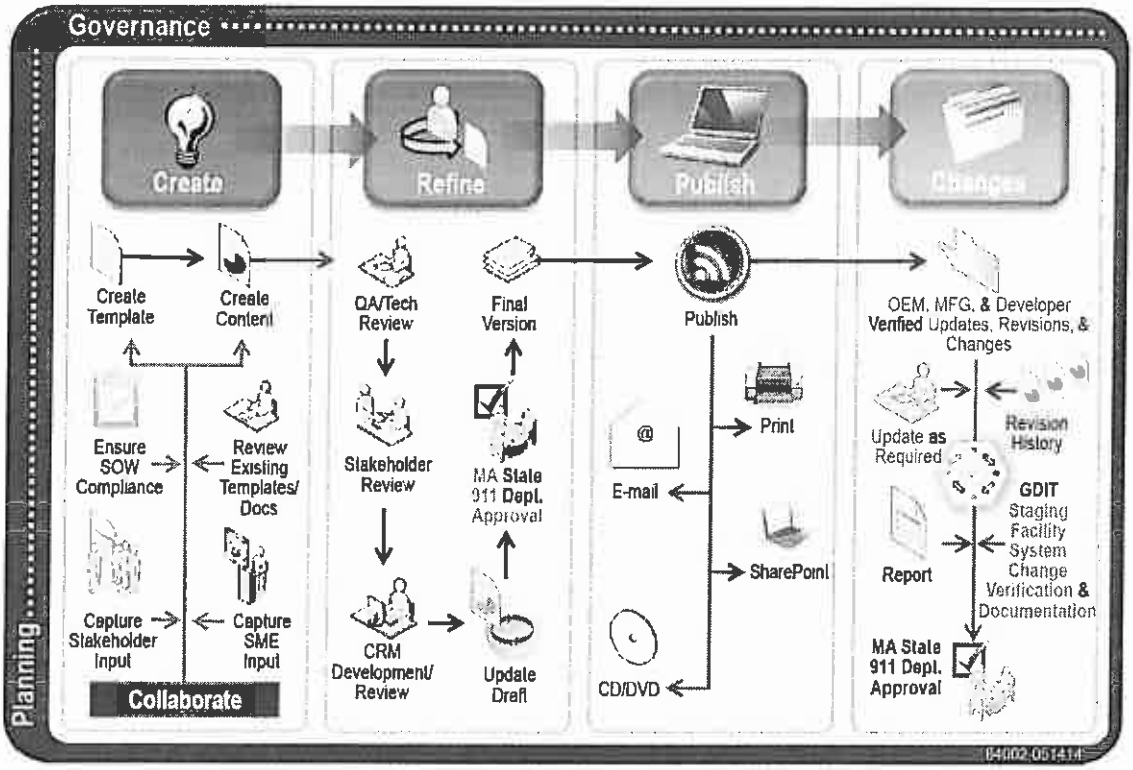


Figure 71. Configuration and Change Management Document Process

GDIT will also develop and accurately maintain a Configuration Management Database (CMDB) to track configuration items that are essential tracking and managing, such as servers, computers, software and hardware, licenses, network devices, and components. This CMDB will be accessible to the State 911 Department.

8.11. SECURITY, ANTI-VIRUS, AND PATCH MANAGEMENT

Bidders shall describe in detail the system's security, Anti-Virus, and patch management processes. The contractor shall maintain security patch management, Anti-Virus, Anti-Spam, and Anti-Malware processes and products. The contractor shall also maintain an intrusion protection service/intrusion detection service pro-active threat detection solution for security threats.

GDIT will comply with the RFR specification.

Our collaborative approach to MA NG9-1-1 system security will harnesses innovation, hardened processes, synergies, and expertise across our company's longstanding history of delivering security solutions for our customers. In addition, we will provide the Commonwealth the experience of being "the leading cyber security contractor" in the federal marketplace according to FedSources, a Washington-based consultant (now Deltek). In 2013, General Dynamics generated over $2B in cyber portfolio revenue designing, operating, and sustaining our nation's most sensitive networks and critical missions. Our objective is to become an integral partner within the Commonwealth of Massachusetts and the MA NG9-1-1 opportunity and to help the Commonwealth achieve their security goals and to assist in delivering a secure, integral network environment.

GDIT understands the security requirements as prescribed by the MA NG9-1-1 RFR. We have proposed a security solution that satisfies all security requirements and have verified our solution against the NENA 75-001 Security Guideline and the Criminal Justice Information Services (CJIS) Security Policy for compliance. Additionally, all MA NG9-1-1 security requirements were satisfied against the backdrop of supplemental industry standards and guidelines, such as National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), that we commonly use to deliver security solutions for similar environments. GDIT maintains an experienced team of security architects, cyber-analysts, and administrators that can establish and maintain cybersecurity operations through best practice approaches prescribed by NIST, DISA, and FISMA. In the following pages, GDIT has proposed a detailed security solution for the MA NG9-1-1 system that incorporates processes, people, commercial tools, and our internal corporate security procedures for delivering a Network Security System that includes (but is not limited to):

- Anti-Virus and Patch Management
- Security Procedures and Information Assurance Process Governance
- Software Integrity Controls
- Encryption
- Authentication, Authorization, and Accounting
- Intrusion Prevention and Detection
- Disaster Recovery/Business Continuity

8.11.1. Anti-Virus and Patch Management

The contractor shall test, validate, install, and manage an anti-virus application in accordance with procedures to be mutually agreed upon by the parties. The response shall describe the proposed Anti-Virus application and shall describe the proposed processes and procedures for the installation and management of the Anti-Virus application. The mobile PSAP is inactive between deployments, and, therefore, the parties shall, by mutual agreement, schedule the Anti-Virus updates for the mobile PSAP at a mutually agreeable date and time.

The contractor shall identify, test, validate and install updates no less than once per quarter. The contractor shall monitor industry and manufacturer specific notifications for security vulnerabilities and other software and firmware anomalies and apply appropriate measures to eliminate or mitigate such issues in a timely manner following established change management procedures.

The contractor shall, within sixty (60) days following contract award, submit a customized security plan that addresses the manner in which the contractor's security, Anti-Virus, and patch management processes shall be applied to the Next Generation 911 system.

The contractor will be required to use Commonwealth data and IT resources. For purposes of this work effort, "Commonwealth Data" shall mean data provided by the Commonwealth and or the State 911 Department to the contractor, which may physically reside at a Commonwealth or State 911 Department or contractor location. In connection with Commonwealth Data, the contractor shall implement commercially reasonable safeguards necessary to:

- *Prevent unauthorized access to Commonwealth Data from any public or private network;*
- *Prevent unauthorized physical access to any information technology resources involved in the development effort;*
- *Prevent interception and manipulation of Commonwealth Data during transmission to and from any servers;*
- *Deploy a centralized reporting and monitoring tool;*
- *Provide daily definition updates to the Anti-Virus, Anti-Spam and Anti-Malware solution; and*
- *Deploy a network and CPE auditing tool.*

The contractor shall represent and warrant as follows:

- *All media on which contractor provides any software shall be free from defects;*
- *All software delivered by contractor under shall be free of Trojan horses, back doors, and other malicious code; and*
- *The contractor has obtained all rights, grants, assignments, conveyances, licenses, permissions and authorizations necessary or incidental to any materials owned by third parties supplied or specified by the contractor for incorporation in the deliverables to be developed.*

GDIT will comply with the RFR specification.

The MA NG9-1-1 anti-virus and patch management process will be part of an overall vulnerability management activity incorporating people, automated tools, and standards and best practices that will:

- Establish elements for successful and proactive patch management actions that take care of anti-virus signature updates, OS security patching, and hotfixes that apply to the MA NG9-1-1 system.
- Help ensure the availability and reliability of MA NG9-1-1 supporting systems for business continuity.
- Reduce manual system administrative activities and delays commonly associated with performing software updates.

All routine anti-virus, patch management, and administrative system changes performed against MA NG9-1-1 systems comply with Sections 7.4.3, 7.4.4, 7.4.5, and 7.4.6 of the NENA 75-001 System Security Guideline and with Section 5 of the Criminal Justice Information Services (CJIS) Security Policy. Through our experience, GDIT has delivered cybersecurity solutions, including the design, implementation, and maintenance of vulnerability management systems across a broad array of engagements throughout the federal government and DoD over the last 15 years. Our team will carry that experience forward to the Commonwealth of Massachusetts and apply it to supporting the vulnerability management mission for MA NG9-1-1.

The MG NG9-1-1 anti-virus and patch management process will baseline all supporting network elements and systems in order to maintain the highest level of security and integrity and will incorporate each component into the vulnerability management life cycle as illustrated in Figure 72. The vulnerability management life cycle includes the following elements, and is used to establish:

- **Policy** – for secure computing and patch management, standards, software updates, specifications, and risk acceptance.
- **Baseline** – for defining the application portfolio, network attack surface, and inventory.
- **Priority/Assessment** – for use in determining business risk and prioritizing remediation efforts.
- **Protection** – for developing custom rules and workflows to detect and block exploitation attempts against MA NG9-1-1 systems.

- **Mitigation Strategy** – for communicating business risk and compliance implications of vulnerabilities; for patching during routine intervals; for scheduling/staffing resources as required or available; for establishing a procedure for out-of-cycle patching of serious vulnerabilities (i.e., zero-day attacks, advanced persistent threats (APCs), etc.)

- **Root Cause** – for understanding the nature, behavior, and origin of the vulnerability that can be used for future analysis/postmortem, mitigation planning, and reporting.

- **Reporting and Metrics** – for establishing risk ratings and density; determining security vulnerability history and trending; for compliance-based analysis, forensics, reporting, and situational awareness.

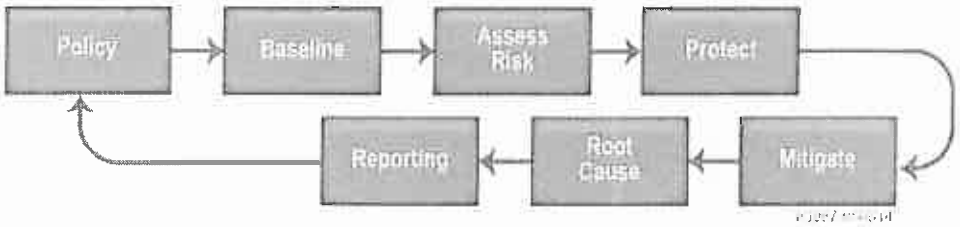


Figure 72. Vulnerability Management Cycle

Anti-virus and patch management activities will be performed from the GDIT Security Operations Center (SOC) center located in Needham, MA. Routine host scans will be performed against all MA NG9-1-1 systems at each subsystem location including PSAPs, data centers, and NOC/SOC locations in order to determine and satisfy baseline compliance. All patches and updates will be verified against Microsoft security patch release and McAfee data file (.DAT) installation instructions, MA NG9-1-1 Security Policy, and any functional system integration dependencies required of the MA NG9-1-1 system. The MA NG9-1-1 anti-virus and patch management policy will apply to all network and computing systems to ensure compliance, security governance, and system integrity.

GDIT's anti-virus and patch management system will be comprised of the following main components to include:

- **Vulnerability Scanner** – AlienVault Unified Security Management™ (USM) will be used to perform five essential security functions (to include vulnerability scanning) as a core component of the MA NG9-1-1 Vulnerability Management System including:

  — *Asset Discovery* – network discovery and inventory

  — *Vulnerability Assessment* – active network scanning, and continuous vulnerability monitoring

  — *Threat Detection* – IDS, host-based IDS (HIDs), file integrity monitoring

  — *Behavioral Monitoring* – to include netflow analysis, and log normalization

  — *Security Intelligence* – Cyber Situational Awareness (CSA) log management, and Security Information Enterprise Manager (SIEM) event presentation, correlation, and filtering

- **Host Protection** – McAfee Endpoint Protection Suite will facilitate all endpoint protection and anti-virus capability for MA NG9-1-1 server systems and client computing elements that will protect against antivirus, antispam, web security, provide host-based firewall, and intrusion prevention capability.

- **Microsoft Updates** – Windows Server Update Services (WSUS) will enable MA NG9-1-1 system administrators to manage the distribution of updates and hotfixes released for all Microsoft products. WSUS can automatically download and make ready all updates required for MA NG9-1-1 Microsoft-based systems.

Our patch verification process will ensure timely provisioning and careful implementation of all security updates, patches, and upgrades. As shown in Figure 73, this sample MA NG9-1-1 patch update process will leverage a controlled patch release process to ensure baseline integrity, with minimal impact to the production system and operations. Laboratory testing and staging of patches will be performed in Needham, MA at GDIT's i3 Solutions Interoperability Lab in support of the MA NG9-1-1 system. This process adheres to our development and quality assurance program discussed in greater detail in Section 8.11.3 (Software Integrity Controls) that effectively segregates activities between our development and staging lab and the MA NG9-1-1 production environment.

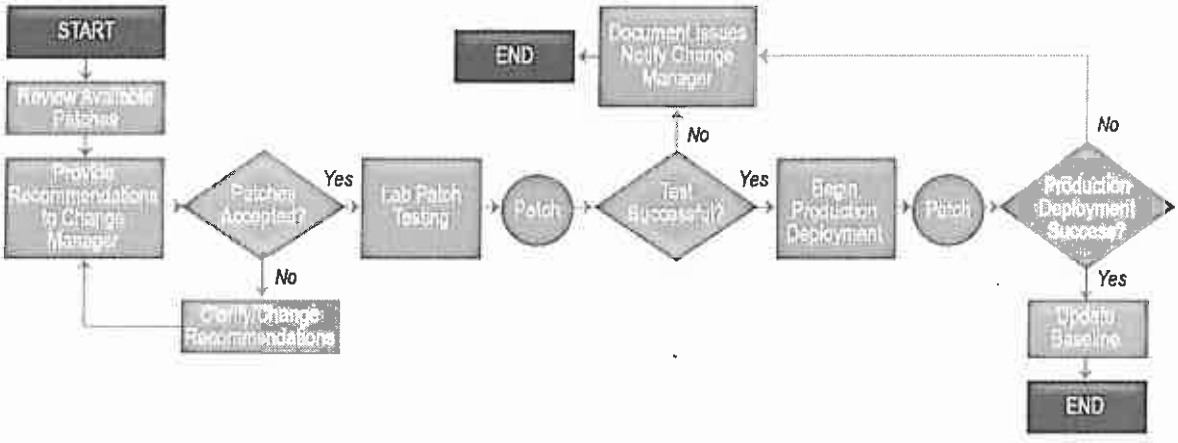


Figure 73. Patch Verification and Update Process

8.11.2. Security Procedures

The contractor shall implement appropriate best-practice security measures that are compliant with any and all applicable federal, state, and local laws, regulations, and guidelines to ensure that the integrity of the system is not compromised.

Bidders shall describe (1) their own and their proposed subcontractors' respective internal security procedures and policies applicable to work performed by them for customers and (2) the particulars of any circumstances over the past five (5) years in which the bidder or its proposed subcontractor(s) has caused a breach of the security, confidentiality or integrity of a customer's data.

Section 6 of the Commonwealth Terms and Conditions states:

"Confidentiality. The contractor shall comply with M.G.L. c. 66A if the Contractor becomes a "holder" of "personal data." The contractor shall also protect the physical security and restrict any access to personal or other State 911 Department data in the contractor's possession, or used by the contractor in the performance of a

contract, which shall include, but is not limited to the State 911 Department's public records, documents, files, software, equipment or systems."

In addition to the foregoing requirements, the bidder must agree that as part of its work effort under the agreement entered pursuant to this RFR, the bidder may be required to use the Commonwealth personal data under Massachusetts General Laws c. 66A and/or personal information under Massachusetts General Laws c. 93H, or to work on or with information technology systems that contain such data in order to fulfill part of its specified tasks. For purposes of this work effort, electronic personal data and personal information includes data provided by the State 911 Department to the winning bidder which may physically reside at a location owned and/or controlled by the Commonwealth or the State 911 Department or winning bidder. In connection with such data, the winning bidder shall implement the maximum feasible safeguards reasonably needed to:

- *Ensure the security, confidentiality and integrity of electronic personal data and personal information;*
- *Prevent unauthorized access to electronic personal data or personal information or any other Commonwealth data from any public or private network;*
- *Prevent unauthorized physical access to any information technology resources involved in the winning bidder's performance of a contract entered under this RFR;*
- *Prevent interception and manipulation of data during transmission to and from any servers; and*
- *Notify the State 911 Department immediately if any breach of such system or of the security, confidentiality, or integrity of electronic personal data or personal information*

GDIT will comply with this RFR specification and will implement best-practice security measures that comply with NENA guidelines, CJIS, NIST, and FISMA to ensure that the integrity of the system is not compromised.

GDIT's corporate internal security procedures and IT governance policies have enabled an extremely secure environment for over 90,000 employees, countless classified artifacts and customer program information, and vital customer financial and contractual data. Our security procedures and the methods by which we execute them are annually reinforced through routine internal and external audits, annual employee training and certification, counter-intelligence training, data import and export compliance controls, and ethics training. As a result, there have been no reported circumstances that have led to any breaches of the security, confidentiality, or integrity of any of our customer's data in the past five (5) years.

GDIT is dedicated to safeguarding our employees, contractors, visitors, facilities, and the environment at all company locations by complying with applicable legislation, regulations, and other requirements. GDIT has a combined Quality, Environmental, Health, and Safety (QEHS) management system that provides the infrastructure and processes to achieve QEHS goals and maintain a culture of continual improvement and security. GDIT maintains compliance with applicable legal and regulatory requirements, and has systems in place to validate and correct security compliance issues when needed. The GDIT QEHS strategy includes:

- Quality Management System (QMS) – GDIT uses the International Organization of Standardization (ISO) 9001:2008 across all business engagements to ensure a consistent quality management system baseline is established and maintained. The GDIT baseline is enhanced by additional standards, models, and frameworks including the Capability Maturity Model Integration (CMMI), Information Technology Infrastructure Library (ITIL); Six Sigma; Project Management Body of Knowledge (PMBOK); Earned Value Management Systems (EVMS); Lean Six Sigma (LSS); and NIST security guidelines as business security needs require. GDIT uses a company-wide multi-site approach for ISO 9001 registration. In this approach, ISO 9001 registration sites include GDIT

headquarters, division headquarters, main offices and all sites (including all sites supporting MA NG9-1-1) that have a contractual requirement for registration. All sites are included in our annual security auditing program.

- The GDIT QEHS management system encompasses the full spectrum of GDIT products and services, including engineering, design, development, fabrication, testing, installation, operation, maintenance, training, and support systems for information technology in commercial, government, and military arenas worldwide.

As a systems integrator with longstanding experience providing solutions to the federal and state governments, GDIT is intimately familiar with federal, state, and local laws, regulations, and guidelines as they apply to securing information systems. GDIT's Needham facility, which will house the MA NG9-1-1 program office and Network and Security Operation Center (NSOC) is audited annually by the Defense Security Service. This is a complete and thorough inspection of clearances, classified systems, security awareness training, counter-intelligence, and our overall security posture. GDIT is consistently rated either commendable or superior during these audits. We will use this experience as well as commercial industry best practices to ensure the integrity of the MA NG9-1-1 system. We have numerous facilities within the Commonwealth that are certified and authorized to perform classified work for the federal government.

We have an extensive set of internal security procedures and policies to ensure all work is performed in a secure and ethical manner. In accordance with our policies, information for this project will be shared internally on a need-to-know basis when it is necessary for the recipient of the information to have the material in order to complete their assigned task.

All data is stored in a manner that precludes access by unauthorized personnel. Information is stored in locked desks or file cabinets or rooms with controlled access. Our Needham facility is only accessible via controlled access. Data maintained in electronic format must be stored in a computer network maintained and controlled by GDIT. Any data maintained outside of the corporate network must be stored on an encrypted device that meets a 128-bit or higher encryption standard.

Security software, including the items below, is provided with all GDIT network computing assets to include:

- Host-based firewall
- Virus and malicious code protection
- ParityBit9
- Security logging
- RSA token with two-factor authentication for remote access

We routinely perform audits on all processes for compliance with our ISO 9001 certification. As stated earlier, all employees are required to obtain annual refresher training on these policies and the methods by which GDIT conducts business. As a term of their employment agreement with GDIT, all subcontractors, temporary hires, and partners are required to understand and adhere to the same standards as GDIT corporate employees.

GDIT understands that as part of the proposed work effort, our team may be required to use Commonwealth personal data under Massachusetts General Laws c. 66A and/or personal

information under Massachusetts General Laws c. 93H, or to work on or with information technology systems that contain such data. As common practice, GDIT will protect this information with as much care as our own company propriety data and personal information of our employees and partners. Our proposed security architecture makes use of industry's best technology to ensure the MA NG9-1-1 system and program assets are not compromised. We will use the appropriate safeguards to ensure the security, confidentiality, and integrity of all Commonwealth personal data. We will utilize a robust authentication process to ensure only authorized personnel have access to any data on the system to include personal data. Our facilities utilize personal access controls and remote monitoring of physical access points to restrict and alert to unauthorized access. All transmissions between physically secured locations will be encrypted to prevent interception and manipulation of data during transmission.

8.11.3. Software Integrity Controls

The contractor shall implement the following software integrity controls for the purpose of maintaining software integrity and traceability throughout the software creation life cycle, including during development, testing, and production.

The contractor shall configure at least two software environments including a development/quality assurance (QA) environment and a production environment.

The contractor shall implement a change management procedure to ensure that activities in the development/QA environment remain separate and distinct from the production environment. In particular the change management procedure shall incorporate at least the following:

Segregates duties between development and testing of software changes and migration of changes to the production environment;

Implements security controls to restrict individuals who have development or testing responsibilities from migrating changes to the production environment; and

Includes a process to log and review all source control activities.

The contractor shall implement a source control tool to ensure that all changes made to the production system are authorized, tested, and approved before migration to the production environment.

The contractor shall not make any development or code changes in a production environment outside of the established change management process.

GDIT will comply with the RFR specification.

As an experienced systems integrator, GDIT maintains state-of-the-art facilities to integrate and test solutions for our customers. These facilities will be utilized to support MA NG9-1-1 to ensure hardware and software delivered to the Commonwealth meets the functional requirements of the project during all facets of development, testing, production, and longer-term maintenance.

We will utilize our i3 Solutions Interoperability Lab facility in Needham, Massachusetts to fully test, evaluate, and stage MA NG9-1-1 subsystems and components prior to releasing them to the production environment. Our lab will have the capacity to contain all components contained within the MA NG9-1-1 production network – both hardware and software. This will support all facets of the MA NG9-1-1 system life cycle that will accommodate for situations related to product obsolescence, technical refresh or modernization, and routine maintenance required by all MA NG9-1-1 hardware and software components regarding system updates, patches, major version upgrades and revisions, and security updates. Our experienced technical support staff and partners will install and configure a logical rendition of the MA NG9-1-1 production environment (separate from the production system) to support these activities. Unless otherwise

directed by the Commonwealth, all changes to the system baseline configuration will be controlled and put through our change management process, signed off and approved by the MA NG9-1-1 Configuration Management team and the system support group prior to production release. The MA NG9-1-1 system support organization is illustrated in Figure 74.

All development and testing in the offline environment will be documented by Level 3 Engineering Support, IA Support, and finally through QA personnel to ensure MA NG9-1-1 system compliance and to confirm system compatibility prior to release. Once completed, all test and release documentation will be delivered and made available to the Commonwealth for additional approvals as required. The MA NG9-1-1 System Support Team and partner engineering staffs will not have access to the production network. All changes to the system baseline will flow through the Configuration Manager, approved, then released to the NSOC support staff, who will apply/implement approved changes only to the production environment.

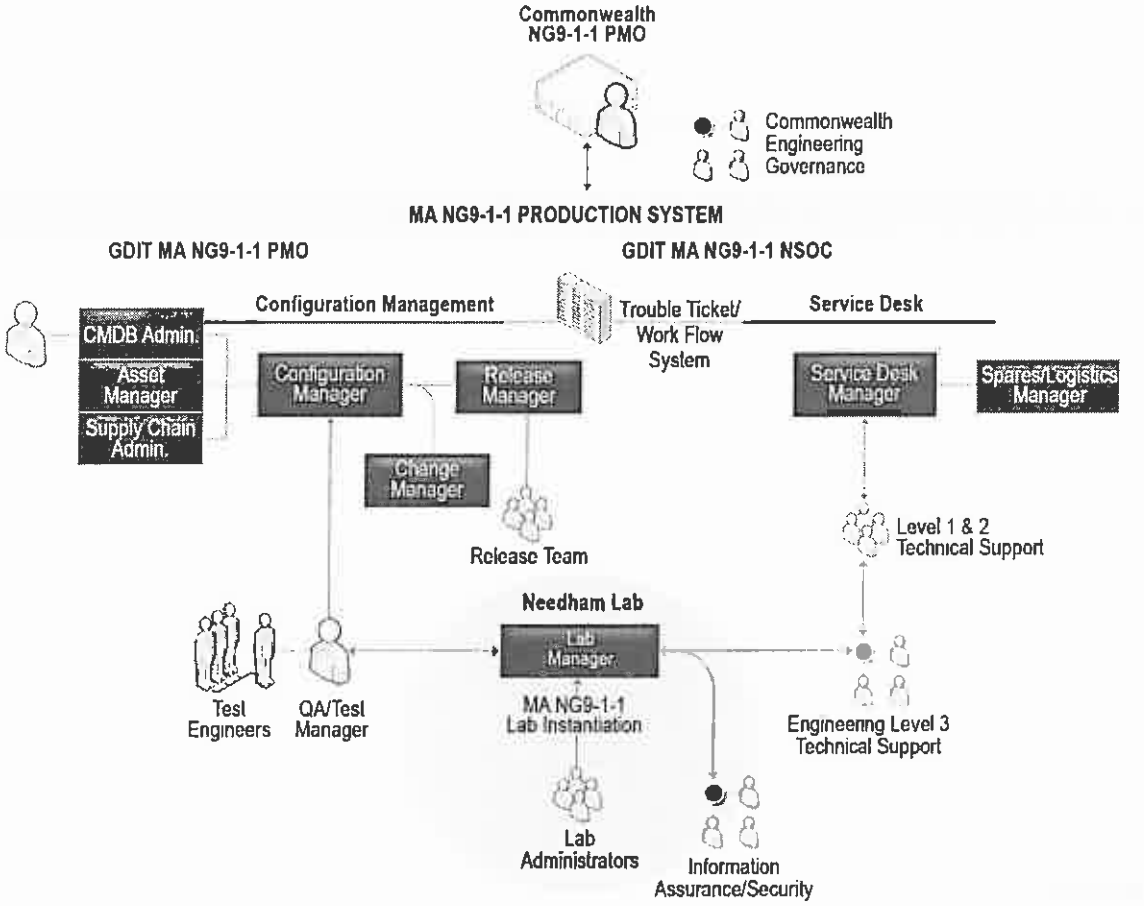


Figure 74. MA NG9-1-1 System Support Organization

Once any change or update is deployed to the production environment, MA NG9-1-1 NSOC personnel will manage the new/upgraded systems to ensure proper functionality. Production change documentation and logs will be generated indicating activities associated with any given production deployment including the devices affected, the original and new configuration baseline, installation, and backout procedures, the time changes were implemented, and any

resulting issues identified during the monitoring period (burn-in). Knowledgebase data and supplemental logs will be provided to the NSOC and system engineering team members to ensure collaboration, history and trending information, and system dependencies. Additionally, this information will be made available to the Commonwealth as required.

Our experience managing and controlling changes to production environments requires strong processes, procedures, and the appropriate staff as indicated earlier. To facilitate workflow automation and the development of a supporting knowledgebase for MA NG9-1-1, GDIT will leverage our automated incident and workflow system, which is comprised of the BMC Remedy IT Service Management (ITSM) suite. We use Remedy internally and have used it primarily for configuration and change management, and workflow. The BMC Remedy ITSM tool, coupled with our processes, procedures, and people will help ensure that all changes to the MA NG9-1-1 production environment are authorized, tested, and approved prior to release and provides evidence of the individuals providing information and approvals should there be a need to relook at the approval process of any given change or workflow order.

As an experienced systems integrator, GDIT maintains state-of-the-art facilities to integrate and test solutions for our customers. These facilities will be utilized to support MA NG9-1-1 to ensure hardware and software delivered to the Commonwealth meets the functional requirements of the project during all facets of development, testing, production, and longer-term maintenance.

8.11.4. Encryption

The contractor shall apply encryption on all communications to ensure that data cannot be viewed or modified by anyone other than the intended recipient, that data can be validated to confirm its source, and to protect the integrity of a message, ensuring that data is complete and unaltered after being transported over the network. The contractor shall describe the method, version, and practical use of the data encryption standard being offered. The contractor shall supply, monitor, and maintain the encryption services.

GDIT will comply with the RFR specification.

The MA NG9-1-1 system will leverage encryption on all communications to ensure that data cannot be viewed or modified by anyone other than the intended recipient as prescribed by the MA NG9-1-1 RFR. To satisfy this requirement, encryption will be applied to the network transport architecture. GDIT will configure Virtual Private Network (VPN) tunneling between each PSAP location and each data center using the integrated VPN encryption engines on the edge routers at each site. In this configuration, we propose the AES-256 advanced encryption standard, which uses a 256-bit key on all communications between locations and will ensure the security of transmissions between locations by ensuring no one is able to decipher the information should they gain access to the transmitted data. The encryption standard is FIPS 197 compliant, ensuring compatibility with other VPN solutions. Additionally, communications by remote users to the data centers will utilize a client-based VPN, which also utilizes AES-256 encryption to ensure that only communications from authorized sources can access MA NG9-1-1 resources if required.

These VPN connections will be monitored and managed from the NSOC using a centralized Security Manager for managing a multi-device, multi-platform VPN, firewall, and Intrusion Detection System (IDS) configuration. The manager allows these security devices to be configured and managed with an easy-to-use Graphical User Interface (GUI). It simplifies the configuration of complex VPN and security devices by creating each device's configuration file

after the security policies have been defined. The Security Manager also distributes each device's configuration in a secure fashion with IPsec. It allows security devices to be configured from a central location, and it also provides other management services including monitoring, notification, and reporting.

8.11.5. Authentication, Authorization and Accounting

The contractor shall ensure that the system employs authentication, authorization, and accounting for controlling access to computer resources and networks, enforcing policies, and auditing usage. Bidders shall describe the authentication, authorization, and accounting functions. The authentication services shall verify the identity of a user before granting access to the network or to any shared resource on the network. The user authentication shall be through a digital certificate, digital signature or password.

The contractor shall ensure that the system employs authorization services that define what users can do once authenticated and that ensures that, after users have been successfully authenticated, they are granted access to only those resources and can perform only those functions that their security credential provides.

The system shall employ accounting services that measure the resources a user consumes during access to include, but not be limited to, the amount of system time or the amount of data a user has sent and/or received during a session.

GDIT will comply with the RFR specification.

Our solution provides for a comprehensive Authentication, Authorization and Accounting (AAA) function using multiple systems to ensure the integrity of system resources. We will deploy a Microsoft Active Directory (AD) domain as the core of the AAA functionality. AD will control access to computer resources and the MA NG9-1-1 network, enforce established security policies, and log usage of system resources. To extend the security of AD, we will integrate the NG9-1-1 domain with a third-party Certificate Authority (CA) and establish domain controllers as subordinate CAs. With this functionality, Public Key Infrastructure (PKI) certificates that can be verified independent of the NG9-1-1 system will be used to provide a higher level of authorization and control over network and system resources. Additionally, we will use an Access Control Server integrated with the AD domain to provide AAA functionality for applications and devices that do not natively support AD or PKI. Finally, we will use independent username/password credentials for any application or device that cannot natively use any previously mentioned functions. In all cases, GDIT will work with application and device developers to include PKI functionality into future releases of their solutions to ensure a fully integrated and capable AAA system.

As a core function of AD, once authenticated to the AD domain, users will be granted access only to resources required to perform their duties. To the greatest extent possible, AD will utilize a role-based access methodology where users are grouped by like functions to ease the administration of user access control management. The system accounting functions will be configured to monitor and record all functions performed by users who have been authorized access to the system resources.

8.11.6. Intrusion Prevention and Detection

The contractor shall provide active intrusion detection services to inspect general network traffic. The system shall, if a pattern of communications associated with network intrusion is detected, create a log and an alert shall be issued to the network service provider and to the State 911 Department. The intrusion detection system shall initiate specific responses to certain perceived threats such as blocking traffic or disabling an account after repeated attempts to log in using an incorrect password. In addition, the contractor shall work cooperatively with the State

911 Department and an independent third party, to be selected by the State 911 Department, for intrusion testing throughout the term of the contract and any renewal thereof.

GDIT will comply with the RFR specifications.

The MA NG9-1-1 Intrusion Prevention and Detection solution will be designed to actively inspect, report, and block malicious traffic. It will be configured to log and notify network defenders when and if a pattern of communication associated with any form of malicious network intrusion is detected. The MA NG9-1-1 Network Intrusion Detection System (NIDS) architecture will house NIDS sensors within each edge router at every PSAP and SOC location (through the Cisco Security Bundle). NIDS capability for each data center will be provided by and configured through the Cisco ASA Firewall. All NIDS sensor devices will be managed by the Cisco Security Manager platform that will be used to receive, normalize, and filter security information generated by the NIDS sensors. Cisco Security Manager helps to enable consistent policy enforcement and rapid troubleshooting of security events, offering summarized reports across the MA NG9-1-1 security landscape. Cisco Security Manager also provides a one-to-many management capability allowing the manager to push new configurations, policy updates, and NIDS signatures to all NIDS sensors simultaneously through the MA NG9-1-1 environment. Cisco Security Manager will be configured to forward security information it receives to the SOC Security Information Event Manager (SIEM) as illustrated in Figure 75. The MA NG9-1-1 NIDS capability will provide:

- Proficiency in detecting intrusions at the MA NG9-1-1 boundary level, and will defend against zero-day attacks with over 40 engines and 6,500 stateful, vulnerability-based signatures that protect against tens of thousands of current exploits – and will be routinely updated to protect against future exploits
- Strong policy-based capability to execute automated responses, and the ability to deal with larger volumes of data (higher capacity) at each boundary location

Each NIDS sensor will actively monitor all network traffic within its respective location for malicious network activity and, if identified and configured with the appropriate response action, will have the capability to automatically block malicious threats as required.

Additionally, all PSAP, SOC, and Remote workstations will utilize local host-based IDS (HIDS) capability to protect the operator workstation from potential threats. The HIDS component is comprised of McAfee Endpoint Protection Suite.

In every case, security alerts and all identified malicious activity within the MA NG9-1-1 environment will be forwarded to the SIEM located at the NSOC. The SIEM is part of the NSOC Security Monitoring platform that will be configured to alert appropriate personnel at the State 911 Department once a threat has been validated by security operators. GDIT will comply with the requirement to work cooperatively with the State 911 Department and an independent third party for intrusion testing throughout the term of the contract. GDIT welcomes the opportunity to verify the security posture of the NG9-1-1 system, and we will take all necessary actions to improve on that security if weaknesses are identified.

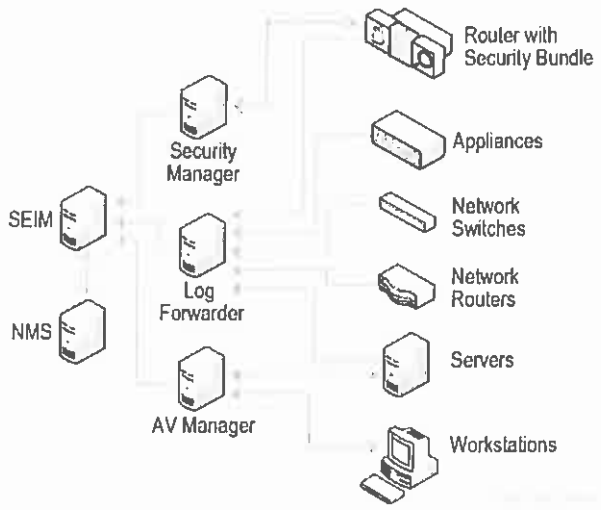


Figure 75. Security Monitoring Platform

- **Cisco Security Manager** – The Security Manager provides visibility and management of the NIDS, firewalls, and VPN functions included in the Cisco routers deployed throughout the NG9-1-1 network. It provides a one-to-many interface to allow instantaneous updates to configurations across the enterprise.

- **Splunk Universal Log Forwarder** – The Splunk Universal Log Forwarder will be configured as a local SYSLOG aggregation and forwarding mechanism that will collect local application log files, capture the output of status commands, extract performance metrics from virtual or non-virtualized sensors, and will monitor local Windows file system logs for configuration, permissions, and attribute changes. The Splunk Log Forwarder will index the messages with a standardized timestamp to aid in forensic analysis, and will forward to the SIEM.

- **McAfee ePolicy Orchestrator (ePO) Anti-Virus Manager** – The ePO Antivirus Manager provides a centralized management capability for monitoring all McAfee endpoint clients installed and operating on Windows servers and workstations. It provides a one-to-many deployment capability for distributing agent policy and .DAT signature updates across the entire MA NG9-1-1 network environment. Additionally, the AV Manager is used to manage desktop intrusion detection, and personal firewall settings on all PSAP workstations and hosts.

- **AlienVault SIEM** – AlienVault will be configured to collect, correlate, filter, and present security information and logs generated by security devices, production servers, and workstations as well as firewall logs and IDS alerts to perform intelligent reporting and root cause analysis. AlienVault will provide an integrated picture and risk status of the NG9-1-1 system. The AlienVault Security Monitoring platform will be used by security analysts to monitor, analyze, respond, and remediate security incidents within the system.

8.11.7. Disaster Recovery/Business Continuity

The contractor shall develop and submit to the State 911 Department for approval, on or before the date of deployment of the first pilot PSAP, a disaster recovery/business continuity plan. The plan shall be invoked in the

event of a catastrophic failure or all or a significant portion of the system. Bidders shall state whether there is a backup NOC and/or a backup help desk, and if so, shall identify the location of such backup facilities. The disaster recovery plan shall address, at a minimum, the following:

- *Persons and entities to be notified;*
- *Message(s) to be conveyed;*
- *Actions to be undertaken by the contractor in an attempt to mitigate the failure;*
- *Roles, responsibilities, and chain of command for mitigation actions;*
- *Recovery and restart procedures after the cause of the failure has been determined; and*
- *Alternative methods of monitoring or determining the status of the network service should the failure limit the contractor's normal methods of monitoring.*

GDIT will comply with the RFR specifications.

GDIT has a proven history of implementing and sustaining mission-critical networks where every contingency must be considered and detailed plans built to address potential service interruption. We will leverage our proven best practices and experience to support the MA NG9-1-1 Department in an approach that will integrate with the State 911 Department's facility, methodology, and practices. Once the Disaster Recovery/Business Continuity (DR) Plan is developed and submitted before the deployment of the first PSAP pilot and approved by the Commonwealth, our workflow will reflect our commitment to providing continuity of operations in response to any events of catastrophic or significant failures.

At an absolute minimum, our DR Plan will also include

- Personnel Notification List (persons and entities to be notified)
- Message(s) to be conveyed
- Actions to be undertaken by the contractor in an attempt to mitigate the failure
- Roles, responsibilities, and chain of command for mitigation actions
- Recovery and restart procedures after the cause of the failure has been determined
- Alternative methods of monitoring or determining the status of the network service should the failure limit the contractor's normal methods of monitoring.

Upon contract award, GDIT will develop the DR Plan using our time- and customer-proven processes aimed at clearly identifying the critical facets such as failover locations, activities/processes, and situational analysis that spans from initial notification through full reconstitution. The DR Plan will ensure our ability to respond to any catastrophic emergency well within the requirement. Additionally, our approach to achieving a resilient, survivable, and redundant architecture is found in Section 8.3 (ESInet) and 8.7 (Next Generation 9-1-1 Architecture).

GDIT's DR Plan leverages our resources, people, and Operations and Maintenance (O&M) processes to ensure catastrophic events are managed and resolved in an expeditious manner. Our approach will employ our Help Desk and NSOC located in Needham, MA as the primary centralized coordination center for all customer and system support and DR activities. This facility has immediate and unlimited access to all GDIT Subject Matter Experts (SMEs),

including Tier I/II/III engineers, site and dispatch maintenance personnel, OEM partners, systems architecture engineers, and executive management. The Help Desk will be co-located with the NSOC and backed up by our secondary GDIT Help Desk and NOC located in Fairview Heights, IL and our secondary SOC in Herndon, VA. Our 24x7x365 operated Help Desk and NOC located in Fairview Heights, IL supports USAF installations and bases located at CONUS and OCONUS locations for telecommunications system technical support and logistics support, such as emergency engineering dispatch, and repair and return of failed components or systems. This also includes providing the same support for nearly 100 E9-1-1 PSAP systems within the USAF. Additionally, the GDIT Help Desk and NOC also provide the same support to entire Federal Aviation Administration (FAA) with more than 900 locations throughout the U.S. Our FAA program also provides disaster response and recovery support.

As spare equipment availability is an important element of a solid DR Plan, we will pre-position all critical spare equipment at our Needham, MA Help Desk and NSOC as part of our DR kit. Additionally, critical spares can be pre-positioned at key locations with Massachusetts to ensure readiness and timely response even for non-emergency system failures. Our long-standing relationship with all major telecommunications and IT OEMs translates into immediate response and premium availability of critical components whenever disaster strikes.

In the following subsections we present a Draft Disaster Recovery/Business Continuity Plan.

DRAFT DISASTER RECOVERY PLAN (DRP)

Purpose

The principal objective of a Disaster Recovery Plan (DRP) is to develop, test, implement, and document a well-structured and easily understood plan that will help the MA NG9-1-1 data centers recover as quickly and effectively as possible from unforeseen disaster or emergency that interrupts information systems and business operations. Additional objectives include the following:

- Ensure all employees fully understand associated duties with implementing the DRP.
- Ensure the Data Center recovery is consistent with the overall recovery of NG9-1-1. The system architecture plays a part in the high availability and recoverability of the system.
- Ensure operational policies and procedures that impact recovery are appropriately documented and adhered to in all planned activities.

Scope

This document is intended for all personnel roles described throughout this document.

Key Personnel Contact Information

Table 16 lists contact information for MA NG9-1-1 key personnel.

Table 16. Key Personnel Contact Information

Name and Title	Contact Option	Contact Number
Joan Newlon, GDIT Project Director	Work Mobile E-mail Address	781-400-xxxx 781-424-xxxx Joan.Newlon@gdit.com
Paul Chotkowski GDIT Project Manager	Work Mobile E-mail Address	781-400-xxxx 781-727-xxxx paul.chotkowski@gdit.com
Stephen Woodworth Contract Manager	Work Mobile E-mail Address	781-400-xxxx 781-910-xxxx Stephen.woodworth@gdit.com

Internal Notification Contacts

The following Commonwealth personnel can be contacted in the order listed:

a. Contact Name, Contact Title/Organization, Contact Project Role
b. Contact Name, Contact Title/Organization, Contact Project Role
c. Contact Name, Contact Title/Organization, Contact Project Role

Plan Overview

Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. When changes are made to the plan, they are to be fully tested and appropriate amendments are to be made to the accompanying documentation. This involves using formalized Change Management procedures under the control of Configuration Management.

Plan Documentation Storage

Copies of this plan will be stored in security locations, to be defined by the hosting data center. Each member of the Disaster Recovery Team (DRT) and the Business Recovery Team (BRT) will be issued a compact disc and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

Backup Strategy

The GDIT team backup strategy needs to be decided and further defined. Disk Backup will consist of Nearline Disk Storage (NLS) along with offline storage (Tape).

Risk Management

There are many potentially disruptive threats that can occur at any time and affect the normal business process. GDIT has considered a wide range of potential threats, and the results are included in this section. Each potential environmental disaster or emergency situation has been examined. Table 17 focuses on the level of business disruption, which could arise from each type of disaster.

Table 17. Disaster and Remedial Management

Potential Disaster	Probability Rating*	Impact Rating**	Potential Consequences and Remedial Actions
Flood	4	4	Verify all critical equipment is located on first floor or higher and raised floor. Floodwall exists at the perimeter of data centers.
Fire	4	3	Suppression system installed in the Enterprise IT Center (EITC) and Systems Integration Environment (SIE). Fire and smoke detectors are on all floors.
Tornado	2	2	In case of a catastrophic disaster, full system recovery can occur in the identified time frame in the Service-Level Agreement (SLA) once an alternate site has been identified and an SLA is executed between the Commonwealth and GDIT.
Electrical Storms	2	4	Redundant Uninterruptable Power Supply (UPS) array and auto standby generator is tested periodically and is remotely monitored 24 hours a day, seven (7) days a week. UPS is also remotely monitored.
Acts of Terrorism	5	1	In case of a catastrophic disaster, full system recovery can occur in the identified time frame in the Service-Level Agreement (SLA) once an alternate site has been identified and an SLA is executed between the Commonwealth and GDIT.
Acts of sabotage	5	1	In case of a catastrophic disaster, full system recovery can occur in the identified time frame in the Service-Level Agreement (SLA) once an alternate site has been identified and an SLA is executed between the Commonwealth and GDIT.
Electrical Power Failure	2	4	Redundant UPS array and auto standby generator is tested periodically and is remotely monitored 24 hours a day, seven (7) days a week. UPS is also remotely monitored.
Loss of Communications Network Services	3	4	Two (2) diversely routed <circuit bandwidth of Point of Presence (POP) Suite> trunks into building. Wide Area Network (WAN) redundancy.

**Probability: 1=Very High, 5=Very Low*
***Impact: 1=Total Destruction, 5=Minor Annoyance*

Emergency Response

Plan-Triggering Events

Key trigger issues at either data center that would lead to activation of the DRP are as follows:

a) Total loss of communications.
b) Total loss of power.
c) Flooding of the premises.
d) Loss of the building (partial or total and catastrophic).

Assembly Points

An assembly point is the location where the premises must evacuate to.

Activation of Emergency Response Team

When an incident occurs, the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a quick reference card, containing the ERT contact details to use in the event of a disaster. Responsibilities of the ERT are to:

a) Respond immediately to a potential disaster and call emergency services.

b) Assess the extent of the disaster and its impact on the business, data center, facility, etc.
c) Decide which elements of the DRP should be activated.
d) Establish and manage a DRT to maintain vital services and return to normal operation.
e) Ensure employees are notified and allocate responsibilities and activities, as required.

Disaster Recovery Team

The DRT will be contacted and assembled by the ERT. Responsibilities of the DRT include:

a) Establish facilities for an emergency level-of-service in two (2) business hours of the incident.
b) Restore key services in four (4) business hours of the incident.
c) Recover to business as usual 8–24 hours after the incident.
d) Coordinate activities with DRT, first responders, etc.
e) Report to the ERT.
f) Contact Commonwealth key personnel.

Emergency Alert, Escalation, and Disaster Recovery Plan Activation

This policy and procedure has been established to ensure in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established, while activating disaster recovery.

The DRP will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the facility and system return to normal operating mode.

Emergency Alert

The person who discovers the incident calls a member of the ERT in the following listed order:

a. ERT:
    1. Joan Newlon, GDIT Project Director
    2. Paul Chotkowski, GDIT Project Manager
    3. Stephen Woodworth GDIT Contract Manager, GDIT

If unavailable, contact:

    1. Alternative_Lead_Person, Title/Role

The ERT is responsible for activating the DRP for disasters identified in this plan, as well as any other occurrence that affects the facility's or system's capability to perform normally.

b. During the early stages of the emergency, the DRT is notified that an emergency has occurred.

The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to effectively communicate this request.

The BRT will consist of senior representatives from the main business departments:

The BRT Leader will be a senior member of the Site Management Team, responsible for taking charge of the process and ensuring the site and facility returns to normal working operations as early as possible.

Disaster Recovery Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the facility's DRP and Contingency and Business Continuity Plans (CBCP) on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis and the facility's immediate plans. Employees who cannot reach staff on their call lists are advised to call the staff member's emergency contact to relay information on the disaster.

Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

Recorded Messages and Updates

For the latest information on the disaster and the organization's response, staff members can call a toll-free hotline listed in the DRP wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

Alternate Recovery Facilities and Hot Site

If necessary, the hot site will be activated, and notification will be given via recorded messages or through communications with managers. Hot site staffing will consist of members of the DRT only for the first 24 hours, with other staff members joining at the hot site, as necessary.

Personnel and Family Notification

If the incident has resulted in a situation that would cause concern to an employee's immediate family, such as hospitalization of injured persons, it becomes necessary to notify the employee's immediate family members as soon as possible.

Disaster Recovery Plan Exercising

DRP exercises are an essential part of the plan development process. In a DRP exercise, there is no pass or fail; everyone who participates learns, from exercises, what must be improved and how the improvements can be implemented. Plan exercising ensures emergency teams are familiar with their assignments, and more importantly, are confident in their capabilities.

Successful DRPs launch into action smoothly and effectively, when needed. This will only occur if everyone with a role to play in the plan has rehearsed the role more than once. The plan should also be validated by simulating the circumstances within which it has to work and taking note of the outcome.

8.12. TRAINING

The contractor shall provide the following training services:

The response shall include a comprehensive training plan that identifies the proposed training services, methods, and procedures for the system both during and after the conversion from the legacy system to the Next Generation 911 system.

The contractor shall work cooperatively with the State 911 Department to determine the curriculum content for all training, including without limitation, end user, administrator, and State 911 Department staff training and training materials. The State 911 Department shall have the option to customize training and training materials at all phases of program development for any and all training, including without limitation, end user, administrator, and State 911 Department staff training, and the contractor shall, upon request, review all such training materials for accuracy.

GDIT will comply with the RFR specifications.

The GDIT team is an all-inclusive team and, as such, has aligned the best of all core competencies for this initiative. Due to their expertise and extensive knowledge of NG9-1-1, E9-1-1, and the Commonwealth's deployed infrastructure, we have selected our teammate Winbourne Consulting to provide instructors in support of our training initiatives. Glen Roache of Winbourne Consulting will work directly with the GDIT Learning Center of Excellence (LCOE) to meet all training requirements stipulated in the Request for Response. The close proximity of our training experts to our technical team will not only provide for a cohesive team, but also reduce any unnecessary risks. GDIT's LCOE is an industry-wide recognized and award-winning training group.

GDIT established the LCOE to enable customers to seamlessly adapt and apply the advantages of new learning and teaching paradigms to their performance and training needs. Whether the training need is based on new system implementation, employee performance improvement, or new mission directives, we still believe in, and conscientiously apply, the *Science of Learning and Performance*. This dedication to the goal of improving performance through learning has garnered the GDIT LCOE significant recognition in the industry. Our ability to provide superior performance-based learning products and services is based on our sound (and continually evolving) understanding of both learning and performance principles and methods, our people's outstanding instructional design and human performance competencies and experience, and our linked set of flexible and customizable processes. These elements have qualified GDIT to provide the State 911 Department with the most effective training to successfully meet the goal of implementing the NG9-1-1 emergency communications system in Massachusetts.

Our LCOE is a completely self-contained facility and includes a state-of-the-art 600 sq. ft. video post-production suite with designated areas for video editing, audio production/integration, digitization, and duplication in addition to a recording studio. In addition, our digital media department uses the latest equipment and processes for the production of 2D graphics, 3D animations, immersive learning environments, and avatar technology. Our core expertise includes:

- Web-based and Blended Learning/Training Solutions, Curriculum Development for Instructor-led Training, Interdisciplinary Learning and Teaching (ILT) Train-The-Trainer, Virtual Learning Centers
- Desktop Simulations, Electronic Performance Support Systems (EPSS), Integrated Performance Support Systems (IPSS), and Training and Performance Support System (TPSS)
- Knowledge Management, Digital Training Facilities Management, Learning Management System (LMS) Integration, and Digital Media Production
- Human Performance Assessment, Evaluative Research, Reliability, Validity, Validation Studies, and all phases of Analysis

As a result of GDIT supporting clients such as the Department of Homeland Security (DHS), Department of Veterans Affairs (VA), the Office of Personnel Management (OPM), and the U.S. Navy on a long-term basis, we have been able to foster an experienced workforce that is proficient in our processes and tools. Our team consists of highly skilled personnel in the disciplines of *Instructional Systems Design, Human Performance Improvement, Computer Science, Education and Adult Learning, Audio/Video Services, Project Management, Graphic Arts and Media Design, Industrial/Organizational Research and Assessment, and Instructional Technology*. The technical experts from GDIT, our key subcontractors Synergem, DSS, DDTi, Windstream, Emergency CallWorks, and key OEMs will all be consulted in the development of training materials

With over 250 dedicated training professionals, rapid access to this core training capability enables us to handle many tasks simultaneously across multiple locations if needed. Figure 76 represents our staff's level of education and skills.

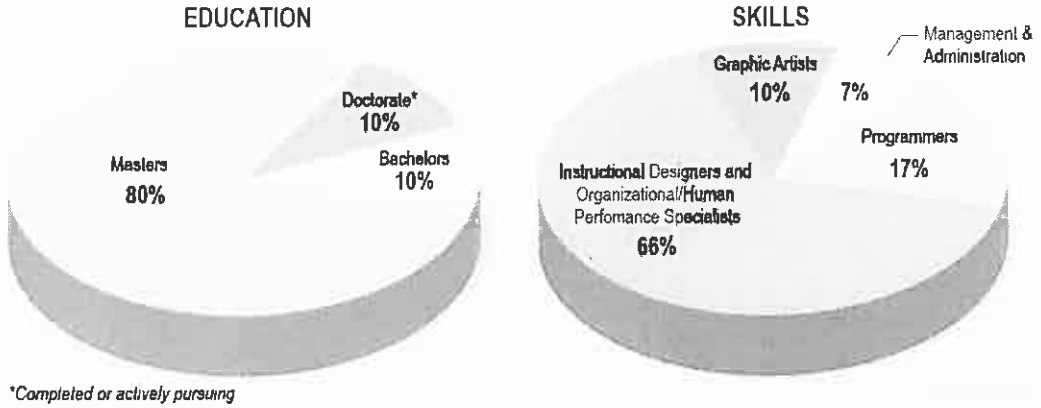


Figure 76. GDIT Staff Education and Skills

Our training experts at the LCOE understand the various training requirements and are ready to begin on Day 1 to support this contract.

8.12.1. Training Material

The contractor shall furnish all software, manuals, and audio/visual aids necessary for training on the system. The contractor shall provide such materials to the State 911 Department in an electronic format specified by the State 911 Department that will permit the State 911 Department to manipulate and edit such materials. Any manuals, software programs and audio/visual training materials created and developed by the contractor shall become the sole and exclusive property of the State 911 Department with rights to copyright and sublicense and shall be subject to the sole and exclusive use, alteration or revision by the State 911 Department. The contractor shall print and distribute all training materials approved by the State 911 Department, including without limitation, the materials that shall be distributed at training classes hosted by the contractor, as directed by the State 911 Department.

8.12.1.1. Overall Design Considerations

GDIT understands that for any successful implementation of state-of-the art systems such as the NG9-1-1 Emergency Communications System for Massachusetts, effective training for the right people involved, at the right time, is crucial. Training should not be an afterthought but a well-planned activity integrated into the overall plan to design, equip, install, operate, monitor, maintain, and support the system. Coupled with this is the fact that the quality of the training program is also crucial to the success of this effort. Quality training requires that the design of the courses apply principles of the Science of Learning so that the intended target audience actually retains what they have learned and are able to perform the tasks of the job at an optimum level of proficiency. This means that just the mere transfer of information doesn't always guarantee that learning occurred. For this reason, our team of Instructional Systems Designers will apply the most effective instructional and teaching strategies to each Program of Instruction (POI) so that the intended audience, the State 911 Department Training and System staff, CPE users, and PSAP administrators maximize their own learning. Below are some examples of teaching and learning strategies that may apply to this type of instruction:

Table 18. Examples of Teaching and Learning Strategies

Instructional Strategies
Work-Situation Simulations: Based on simulation and modeling principles contextualize learning by placing students in authentic simulated situations and requiring them to demonstrate performance of job/task activities using real-world case scenarios systems simulations.
Incorporate **Process Mapping** strategy into the teaching materials to plan and reinforce procedural tasks.
Incorporate the use of high-resolution visuals such as **Authentic Systems-Related Artifacts.** For example, visual presentation of system network architecture and database design for teaching practice and testing.
Incorporate a **Portfolio Toolkit** in the Student Guides that will include job aids and other support tools related to specific procedures and processes.
Provide opportunities for student **Collaboration** through the use of interactive discussion, activities, and practice **exercises.**
Provide opportunities for **Role** Play activities within a simulated live environment.

8.12.1.2. Overall Methodology

In addition to instructional integrity considerations, for each training requirement we implement a comprehensive and well-established systematic development process that has repeatedly resulted in successful performance improvement solutions that meet our customers' training and performance goals. This approach consists of an agile development methodology that includes multiple flexible phases to analyze, design, develop, test, deliver, evaluate, and refine utilizing

the Analysis, Design, Development, Implementation and Evaluation (ADDIE) model to ensure instructional integrity.

Figure 77. GDIT's Development Approach

In collaboration with the State 911 Department stakeholders and system Subject Matter Experts (SMEs), the training team will apply this systematic development process to the three training requirements:

- Operations Training
- Conversion Training
- PSAP Administrator Training

8.12.1.3. Next Generation 911 Training Considerations

For all three training requirements, the following items will be taken into consideration:

- All curriculum materials will be developed and submitted in an electronic format acceptable to the State 911 Department. All source files will be provided so that the State 911 Department will be able to make changes and updates as needed. In addition, for the purpose of *Life Cycle Maintenance (LCM)* of the training program, GDIT will provide a LCM Plan that will detail all material templates, standard formatting, and versioning nomenclature.

- To ensure ease in updating lesson content quickly and effectively, we will apply a *"Plug and Play" approach* so that lesson changes and/or updates can be swapped without negatively affecting the course's Program of Instruction.

- All materials to be developed for the three training requirements will become the sole property of the State 911 Department. All materials branding will reflect the State 911 Department's branding.

- GDIT will be responsible to print and distribute all training materials approved by the State 911 Department and this includes the materials to be distributed at training classes.

8.12.2. Operations Training

The contractor shall present a plan to provide a one (1) day (eight (8) hour) comprehensive training class to train, qualify, and certify as needed the State 911 Department Training and System staff. The number of students per training class shall not exceed five (5) persons. At a minimum, the training shall cover network architecture and functionality, database design and functionality, applications and appliances, CPE end user design, functionality

and operation, and all supporting hardware and software systems. The contractor shall also be responsible for training all State 911 Department Training and Systems staff on any and all functionalities and/or payload types throughout the term of the contract and any renewal thereof.

The scope of the Operations Training development effort includes curriculum development for a one-day, eight-hour classroom session to train, qualify, and certify as needed the State 911 Department Training and System staff. The core area of instruction will include as a minimum:

- Network architecture and functionality
- Database design and functionality, applications, and appliances
- CPE end user design, functionality and operation
- All supporting hardware and software systems

Class sizes for each session will not be more than five (5) participants. This will allow for training for the MA NG9-1-1 staff to be trained at regional training centers or GDIT's Needham NG9-1-1 Center of Excellence. To effectively respond to this training requirement, GDIT will apply its systematic development process to design and develop all the materials necessary to implement this training program. Table 19 summarizes the proposed plan for this effort.

Table 19. Operations Training Plan: Activities in each Phase of ADDIE Model

Phase	Activities	Deliverable(s)
Analysis	• Conduct a thorough CFI analysis to confirm our understanding of the training and learning needs • Develop course's Program of Instruction, which includes the overall structure and sequence of the course including course description and learning objectives, topic outlines, list of lesson topics and modules with measurable objectives, course schedule, and assessment and evaluation strategies.	Course Program of Instruction Document
Design	• Develop templates with branding, nomenclature standards and macros for: – Instructor Guide – Teaching Aids (PowerPoint Slides) – Student Guide – Course Materials Covers	Course Materials Templates with Nomenclature Standards and Macros
Development	• Course content development for: – Course Instructor Administration Section – Lesson Plans – Teaching Aids (PowerPoint Slides) – Glossary – Practice Exercises Answer Keys – Test Package with Answer Keys • Student Guide – Course Student Administration Section – Glossary – Handouts – Practice Exercises	Draft Instructor Guides, Test Package, Practice Exercises Package, Student Guide with Exercises, and Handouts
Implementation	• Prepare train-the-trainer materials • Conduct train-the-trainer session with selected instructors	Train-the-trainer Materials Train-the-trainer After Session Report
Evaluation	• Final review to validate that training products meet GDIT's and the State 911 Department's standards and requirements for content validity and instructional soundness	Final Instructor Guides, Test Package, Practice Exercises Package, Student Guide with Exercises, and Handouts, Course

Phase	Activities	Deliverable(s)
	• Develop Course Materials Inventory • Conduct Pilot Testing (recommended)	Materials Inventory
Delivery	• Generate Gold Camera-ready copy for reproduction of course materials • Ship copies of course materials to assigned locations	Copies of Course Materials as needed.

ANALYSIS

8.12.2.1. Commercially Furnished Information (CFI) Analysis

Following contract award, we will conduct an in-depth examination of all materials provided by the State 911 Department as furnished information. The goal of CFI analysis is to ensure that all source materials needed are available and ready for development activities to begin. Tasks include:

- Matching available materials with the overall content areas to be taught
- Identifying additional CFI or SME input needed to fill content gaps of the overall content areas to be taught
- Ensuring that all source materials reflect the most current tasks and procedures

GDIT will provide an inventory of all source materials provided to ensure accountability and proper disposition of materials at the conclusion of the development effort. The outcome of this analysis will prepare the development team for the next activity in the development process, the development of the course's Program of Instruction.

8.12.2.2. Program of Instruction (POI) Development

GDIT and Winbourne Consulting's training development team will facilitate a working meeting with SMEs from the GDIT team, the Mass NG9-1-1 project team, and key stakeholders either virtually or at a selected location. The purpose of this collaborative meeting will be to develop the overall concept of the course in accordance with the State 911 Department's intended goals. The results of this meeting will enable the training development team to identify instructional strategies and methods of assessment, and develop measurable learning objectives, a content topic outline for each lesson, evaluation methods, learning activities and exercises, and daily course schedule. The outcome following the meeting will be the POI document that will be submitted to the State 911 Department for review and approval.

Review Cycles Recommendation
GDIT will provide and administer an *online collaborative project portal* to facilitate communication and collaboration between all project team members and the State 911 Department stakeholders. The State 911 Department project team and other members will be provided with a secure URL only accessible to members through a login process. The site will be accessible at all times throughout the course of the project. The site will be updated on a weekly basis and its content will grow and develop throughout the life cycle of the project. The project portal will provide the following information: • Project planning to include of projected meetings and events • Project tracking to include status reports, deliverable status, minutes, and meeting outcomes. • Work products to include drafts of Lesson Plans, Slides, Student Guides, etc. • Project review so the State 911 Department can conduct online reviews of products. Feedback, comments, and suggestions will be captured using an online mechanism.

Review Cycles Recommendation
Additional information such as project team member listing, contact information and related links will also be made available per the State 911 Department approval.

DESIGN

8.12.2.3. Materials Templates

At this stage in the process, GDIT will develop course materials templates for the Instructor and Student Guides. These templates will be created using the State 911 Department's approved software. The training development team will create macros and reference icons as appropriate.

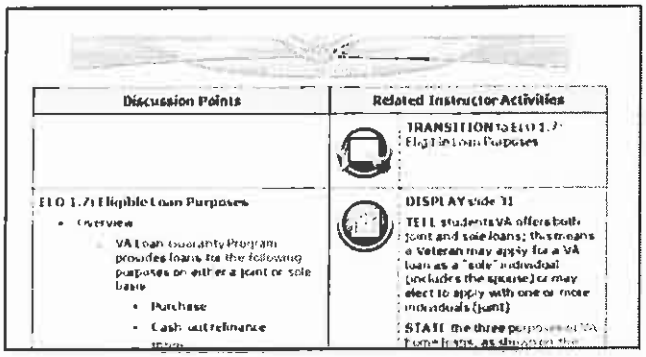


Figure 78. Example of Reference Icons

In addition, we will develop materials covers with an approved State 911 Department branding and nomenclature and versioning standards as post-implementation updates may occur. All the templates will be submitted to the State 911 Department for review and approval.

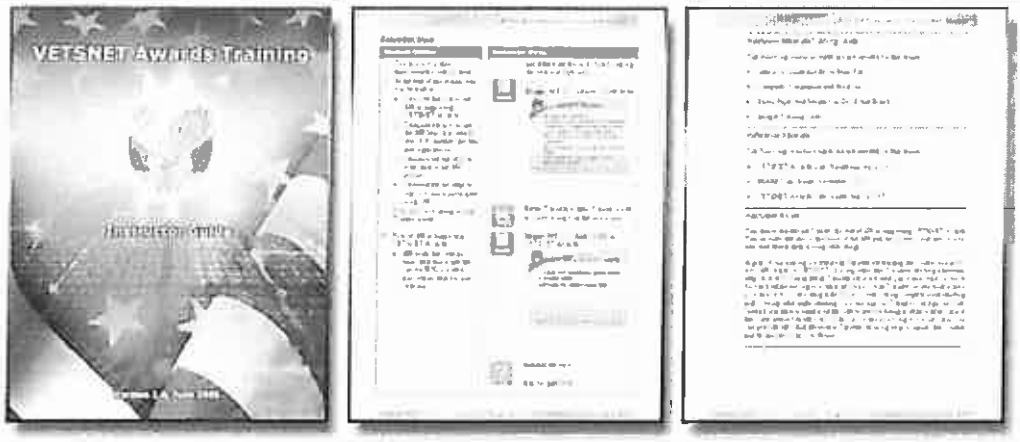
DEVELOPMENT

8.12.2.4. Instructor Guide Development

Based on the training teams experience delivering previous 9-1-1 and other similar courses for instructor-led training, we know it is important to provide a consistent curriculum so that course content is delivered in a reliable manner. Using PowerPoint slides as a sole teaching mechanism is not an optimal method for instructors to deliver effective training, so for this reason, it is important to provide instructors with a complete package that includes a comprehensive Instructor Guide. This Instructor Guide includes several important components formatted in accordance with the State 911 Department's formatting standards:

- Course Instructor Administration Section
- Lesson Plans
- Teaching Aids (PowerPoint Slides)
- Glossary
- Practice Exercises Answer Keys
- Test Package with Answer Keys

VA VETSNET Training Example



Product Description

GDIT developed 48 hours of curriculum materials for instructor led training and a train-the-trainer session on the VETSNET Awards and VETSNET Finance and Accounting System (FAS) software applications. This training provided Veterans Service Representatives (VSRs) and finance employees an introduction to VETSNET as well as thorough steps for completing their position responsibilities, policies, and procedures using the new applications. The project included conducting a learning analysis, developing course materials templates, and developing draft training materials such as a Comprehensive Instructor Guide and Teaching-Aids, Test Package, a Participant Guide and Handouts, and an End-Of-Course Survey Evaluation, GDIT is also currently supporting a web portal that provides access to all up-to-date VETSNET materials. The training materials developed included innovative performance-based instructional strategies through the use learning by doing activities, games, and collaborative application exercises. GDIT also conducted a 3-day train-the-trainer session to familiarize instructors with the course materials prior to the first VETSNET Awards training session. The VETSNET courses are still in use today.

8.12.2.5. Lesson Plans and Teaching Aids Development

In collaboration with SMEs from our key subcontractors and OEMs, the training development team will use the POI information as a baseline to develop the course's lesson plans. The lesson plans will at a minimum address:

- Lesson introduction
- Motivating statement
- Lesson objectives
- Estimated time to complete the lesson
- Method of instruction (e.g., lecture, working group, practical exercise)
- Instructional support required (e.g., training location, equipment, training aids, and materials)
- Course content with instructor note, check-on-learning questions, activities, and reference to teaching aids

Along with the lesson plans, GDIT will develop PowerPoint slides that emphasize important points in the lesson. The slides will also contain pertinent visuals as needed to highlight important procedures.

Visual Aid Recommendation

Through partnership with the State Department Office of Antiterrorism Assistance, or ATA, we produced first-class immersive training for foreign government law enforcement personnel and civilian security forces from various nations throughout four continents designed to enhance their capability to better predict, prevent, respond to, and mitigate the effects of terrorism. GDIT developed 14 instructor-led courses and over 1,000 hours of antiterrorism Instructor-Led Training delivered to a worldwide audience. Course materials and deliverables include program of instruction document, facilitator guide with detailed scripted instruction in a modularized format, participant guide, participant handouts, training aids (PowerPoint slides and other applicable training aids), course schedule, glossary of terms, knowledge and skills evaluations, pre- post-knowledge survey, End-of-Course Report (ECR) and concept equipment list. GDIT also provided expert content specialists and instructors to support all the phases of each course development cycle and implementation. As part of the Instructor Guide package, GDIT embedded video vignettes in PowerPoint slides to convey critical points. *GDIT recommends applying the same method to reinforce important procedures.*

In addition to the teaching aids, GDIT will develop a glossary and other important reference materials for the instructors. The draft lesson plans teaching aids, and references will be submitted to the State 911 Department for review and approval. Once approved, GDIT will produce all graphics and visuals to complete the teaching aids and continue with the other components of the Instructor Guide.

8.12.2.6. Course Instructor Administration Section Development

Once the lesson plans have been developed, GDIT will develop the Administration section of the Instructor Guide. This section includes as a minimum:

- Course's learning objectives
- Administration contact information
- Course schedule
- Access information for simulated software (if available)
- Instructor tips
- Overview of course teaching strategies
- Overview of assessment strategies for certification (if applicable)

8.12.2.7. Practice Exercises Development

In addition to embedded check-on-learning questions and classroom activities, multiple knowledge recall and application exercises will be developed for the course. These practice exercises or capstone exercises will be more formal in nature and will be designed to prepare the students for the post-test. Practice exercises may be designed for individual interaction or for groups for better collaboration, as appropriate for the nature of the content. If this training is implemented in the *Regional Training Centers*, The use of its simulated equipment capabilities to design performance-based exercises will be maximized for the practice exercises. The Instructor Guide Package will also include the practice exercises answer keys, either in form of slides or as a separate handout, depending on the design of the exercise. All practice exercises will be submitted to our SMEs for review prior to submission to the State 911 Department for approval.

8.12.2.8. Test Package Development

GDIT will develop a comprehensive test package that includes a course pretest and a course post-test. The post-test will gauge the level of knowledge/skill transfer from the instructor to the learners. The pre-course knowledge assessment (pre-test) will be used prior to instruction of the course. The purpose of the pre-course assessment is twofold:

1. To serve as a diagnostic instrument for the learners to see how much they already know about the course material
2. To measure the participants' existing knowledge so the instructor can see where he/she must emphasize during the training

Test items will be developed for each of the course's learning objectives. The test items will be matrixed back to the learning objective information and the content from which the question was generated. The test package will also include answer keys and with remediation strategies.

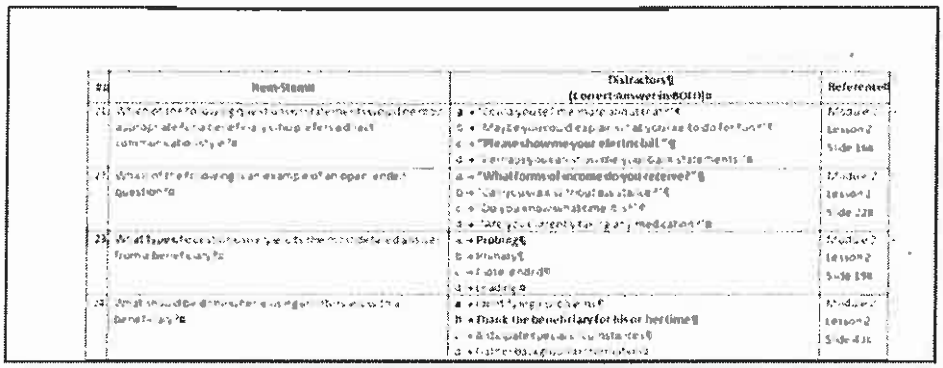


Figure 79. Example of Traceability Matrix

The Test Package will be submitted to SME review then to the State 911 Department for review and approval.

8.12.2.9. Student Guide Development

Once the Instructor Guide has been approved, GDIT will begin the assembling of the accompanying Student Guide that will be based on the content in the approved Instructor Guide. Our development team will format the Student Guide to mirror the Instructor Guide in accordance with the State 911 Department standards. The purpose of the Student Guide is to support course discussions and activities and to enable students to take notes during the course presentation. Following the course, students can use the Student Guide as a resource in addition to any other manuals, texts, or job aids provided in the course. Approval of the Student Guide will complete the Draft Operations Training materials development effort.

IMPLEMENTATION

8.12.2.10. Training the Trainer

To ensure that selected instructors are well prepared to implement this new training, GDIT will create Train-the-Trainer materials in preparation for a Train-the-Trainer session to ensure that the instructor(s) can consistently and effectively teach the course's content. The purpose of the

Train-the-Trainer session is twofold. First, GDIT needs to ensure that the instructors possess the knowledge and skills required to train assigned personnel on all the aspects of the training, and secondly, the instructors possess the instructional expertise to confidently transfer those skills to students. Instructor(s) will be provided with a series of activities that will familiarize them with the course materials. The session will also cover tips and techniques for Instructor-Led Training and provide guidance on classroom preparation and implementation. Upon completion of the Train-the-Trainer session, the participant(s) will be asked to complete a student evaluation survey to capture reactions to the Train-the-Trainer session and materials, including the quality and appropriateness of the content. The data collected will be captured into the Train-the-Trainer Session Report, which will be delivered to the State 911 Department for review and approval.

EVALUATION

During the implementation phase of the project, all course materials will be supplied to the State 911 Department so that a thorough review of the course can be made as a whole. The purpose of this review is to validate that the course meet both GDIT's and the State 911 Department's standards and requirements for content validity and instructional soundness. All comments will be consolidated and the requested changes will be made to complete the final version of the course. It is also at this stage that GDIT will generate a Course Materials Inventory that will be used in future Life Cycle Maintenance efforts for updates and revision. This inventory describes the file names, file descriptions, and version number for all course components.

01_LGY_CLT_Instructor Guide

Sub-Folder Name	File Description	File Name
01_LGY_CLT_IG_Cover_Final	• Instructor Guide Cover	LGY_CLT_IG_Cover_Final.pdf
02_LGY_CLT_IG_Course_Admin_Final	• Instructor Guide Course Administration	LGY_CLT_IG_Course_Admin_Final.doc
03_LGY_CLT_Ducks_Group_Game	• Instructor Guide • PowerPoint – Level 1 • PowerPoint – Level 2	LGY_CLT_Ducks_IG_Final.doc LGY_CLT_Ducks_Level_1_PPT_Final.ppt LGY_CLT_Ducks_Level_2_PPT_Final.ppt
LGY_CLT_Lesson_0	• Instructor Guide • PowerPoint	LGY_CLT_L0_IG_Final.doc LGY_CLT_L0_IG_Final.ppt
LGY_CLT_Lesson_1	• Instructor Guide • PowerPoint	LGY_CLT_L1_IG_Final.doc LGY_CLT_L1_IG_Final.ppt

Figure 80. Example of Course Materials Inventory

Evaluation Recommendation

We recommend that for new courses, a Course Pilot be conducted The purpose of conducting a student pilot is to "try out" the new course using a sample of the student target audience. If a sample is not available, GDIT recommends using the first implementation session as a Pilot. To prepare for a Student Pilot, GDIT will prepare Pilot Execution Plan. The Pilot Execution Plan will include:

- Profile of the target audience
- Formal request for access to the target audience
- Names and qualifications of the GDIT team supporting the pilot
- Recommended process for how to facilitate the Student Pilot
- Recommended process for capturing reaction data
- Recommended process for capturing time tracker Information
- Recommended process for incorporating any changes upon completion of the Student Pilot
- An analysis of the training site, including the classroom and breakout rooms (if necessary)

GDIT will then support the Pilot by observing and recording both student and instructor activities, and capturing

Evaluation Recommendation
reaction data (Kirkpatrick, Level 1) to the training, as well as concerns and issues that may require improvement or correction. This captured data will be discussed with the State 911 Department and instructors to generate a list of approved changes.

DELIVERY

8.12.2.11. Materials Reproduction

GDIT will convert all materials to a camera-ready format for mass reproduction. All training materials will be printed and then distributed to all designated training sites for this course.

8.12.3. Conversion Training

The contractor shall present a plan to provide a one (1) day (eight (8) hour) comprehensive CPE user training class for each enhanced 911 telecommunicator during the conversion from the legacy system to the Next Generation 911 system, including for pilot PSAPs to be identified by the State 911 Department. There are currently approximately six thousand (6,000) enhanced 911 telecommunicators. The contractor shall also provide such additional training as may be requested by the State 911 Department with the cost to be negotiated by the parties, unless costs are identified on Attachment E- Cost Tables.

At a minimum, the training shall consist of all CPE features as they pertain to 911 functionality and operations.

The contractor shall provide a detailed plan on how the contractor shall use mobile remote training systems that shall accommodate up to twelve (12) students in the classroom. The remote training system(s) shall simulate all features of the system as if in a live environment.

The contractor shall provide and deliver training in various areas throughout the Commonwealth to accommodate the deployment schedule. The State 911 Department will be the sole coordinator of all classes and will determine and secure the training locations based on the deployment schedule.

At the request of the State 911 Department, the contractor shall provide refresher training (a four (4) hour class) as necessary to synchronize with the deployment schedule so that enhanced 911 telecommunicators are trained within two (2) weeks of the conversion of the PSAP or otherwise as may be requested by the State 911 Department.

The scope of the Conversion Training development effort includes curriculum development for a one-day, eight-hour classroom session to provide CPE user training for each E9-1-1 telecommunicator during the conversion from the legacy system to the NG9-1-1 system, to include pilot PSAPs identified by the State 911 Department. It is understood that additional training implementations may be needed since it is anticipated that there are currently approximately 6,000 E9-1-1 telecommunicators who need training on the new system. In addition, A four-hour just-in-time module will be developed that will synchronize with the deployment schedule so that E9-1-1 telecommunicators are trained within two weeks of the conversion of the PSAP or upon request.

Training courses will focus on orienting the user with the NG9-1-1 CPE as to overall function, user interface, operations, and capability. Special attention will be paid to provide the users with an easy transition to the new CPE by focusing as well on main function translation, providing a quick reference guide of how the new NG9-1-1 CPE solution crosswalks with the legacy E9-1-1 system's functions. As this is a new user experience, the GDIT team will ensure that each user is not only proficient in the operation of the CPE solution, but has the tools to reference specific capabilities that may have been accomplished in a slightly different manner in the legacy E9-1-1 system (i.e., button names, drop-down menus, etc.).

Conversion training addresses the largest audience (all PSAP staff) and the bulk of the pre-cutover training. This training will be aligned with the migration schedule. Considering there are 254 PSAPs, 104 limited secondary, 3 secondary PSAPs, and 6,000 staff, for planning purposes we have estimated equally; for the larger PSAPs (Boston PD, Worcester, and Framingham for example) with larger staffing loads, we will design final training and schedule accordingly. Using an average staffing load of 4.4 people per shift, per position (24x7 operation), we come to 13.2 staff (on average) per PSAP for a three-position PSAP (average size for planning purposes). There is a population of 3,088 people to train within this size (238 total Primary PSAPs in this class). That load could be addressed in class sizes of up to 25, but in our experience the maximum preferred class size is 20.

Using these figures puts us at 154 classes for conversion for the non-redundant Primary PSAPs. In this example, which accounts for the largest percentage of PSAPs in the Commonwealth, each being one full 8-hour day. Aligned with the rollout schedule, the training team will have full-time training conducted every day (Monday through Friday) in a location serving 20 students. However, as we recognize that class sizes will not ideally be served at this level, we are planning to use the regional training centers in conjunction with the Mobile PSAP to reduce class size, maximize student retention, and diversify geographically. For larger class sessions and more intensive training, the GDIT team will leverage its Needham facilities and its NG9-1-1 Center of Excellence, accommodating larger groups and forums.

As the regional training centers are to be equipped with 10 positions each and, using the Mobile PSAP, we can gain an additional 6, the training team could design an approach to serve 16 people at one location, and 10 at the other 3. However, as the Mobile PSAP is a self-contained unit more suitable for use in rural areas, we will plan to utilize it concurrently to gain efficiencies in rural regions. Using the regional training centers and the 6-position Mobile PSAP, which will all be equipped with the NG9-1-1 call taking solution and, aligning training based on the rollout and clustered migration model, all training can be effectively completed in one calendar year. This model will allow us to serve 26 people (10 per regional training center plus 6 via Mobile PSAP) per day, 130 per week, 6,760 per year (far above the required 6,000 staff requirement).

Accounting for redundant Primary PSAPs with larger staffing loads as well as the limited secondary PSAPs, this class size and ongoing training model will allow the training team to optimally serve the Conversion as well as Operations and Administrator training requirements of the Commonwealth without requiring additional facilities to be equipped.

Note that these calculations are strictly for planning and logistics purposes at this stage, but they exhibit how we will approach the training process overall, accounting for the 6,000 staff.

As with the Operations Training requirement, the systematic development process will be applied to design and develop all the materials necessary to implement this training program to include the refresher training module. Table 20 summarizes the proposed plan for the Initial Conversion Training.

Table 20. Conversion Training Plan

Phase	Activities	Deliverable(s)
Analysis	• Conduct a thorough CFI analysis to confirm our understanding of the training and learning needs • Develop Course's Program of Instruction which includes the overall structure and sequence of the course including course description and learning objectives, topic outlines, list of lesson topics and modules with measurable objectives, course schedule, and assessment and evaluation strategies.	Course Program of Instruction Document
Design	The same templates that were approved by the State 911 Department for the Operations Training effort will be utilized	Course Materials Templates with Nomenclature Standards and Macros
Development	• Course content development for: – Course Instructor Administration Section – Lesson Plans – Teaching Aids (PowerPoint Slides) – Glossary – Practice Exercises Answer Keys – Test Package with Answer Keys • Student Guide – Course Student Administration Section – Glossary – Handouts – Practice Exercises	Draft Instructor Guides, Test Package, Practice Exercises Package, Student Guide with Exercises, and Handouts
Implementation	• Prepare train-the-trainer materials • Conduct train-the-trainer session with selected Instructors	Train-the-trainer Materials Train-the-trainer After Session Report
Evaluation	• Final review to validate that training products meet GDIT's and the State 911 Department's standards and requirements for content validity and instructional soundness • Develop Course Materials Inventory • Conduct Pilot Testing (recommended)	Final Instructor Guides, Test Package, Practice Exercises Package, Student Guide with Exercises, and Handouts, Course Materials Inventory
Delivery	• Generate Gold Camera-ready copy for reproduction of course materials • Ship copies of course materials to assigned locations	Copies of Course Materials as needed.

Similar course materials will be created that will yield to a comprehensive and instructionally sound Conversion Course using the *"Plug and Play"* approach.

8.12.3.1. Use of Mobile Remote Training Systems

GDIT understands that mobile remote training systems will be available for the implementation of this training. We are quite familiar with the existing mobile solutions. With that in mind, demonstration activities will be developed as part of the course's lesson plans. In addition to these demonstration activities used as a teaching mechanism, GDIT will also develop practice exercises to simulate tasks to be complete in a live environment. The practice exercises will be design around role-play strategies and collaborative strategies as applicable to the nature of the tasks to be addressed. Additionally, our training experts will leverage the Mobile PSAPs provided by the Commonwealth to optimize training and regional delivery, outfitting each Mobile PSAP with the new NG9-1-1 call taker application. Depending upon the Commonwealth's desires, this application can be run on existing hardware or installed parallel to

the E9-1-1 system, allowing the Mobile PSAP to be used in the same capacity PSAPs and users are accustomed to today. As the NG9-1-1 call taker workstation is web-client based, access can be established from the existing workstation hardware to the NG9-1-1 simulated environment should the Commonwealth desire. Use of the Mobile PSAPs will allow for expanded training sessions to occur, demonstrations to be done in advance of training, and in-depth customized training for specific PSAP roles in a cost-effective, geographically centric delivery forum.

8.12.3.2. Training Delivery

As part of this contract, this training course will be delivered in multiple areas throughout the Commonwealth to accommodate the approved deployment schedule. GDIT will collaborate with the State 911 Department as the department will be the sole coordinator of all classes and will determine and secure the training locations based on the deployment schedule. A pool of instructors will be available if the need arises that training will be delivered at multiple locations within the same time frame.

8.12.3.3. Refresher Training

GDIT understands the criticality of providing refresher training that is synchronized with the deployment schedule so that E9-1-1 telecommunicators are trained within two weeks of the conversion of the PSAP, so for this reason we will create refresher training to meet this need. The four-hour refresher course will include strategies to recall and reinforce previously acquired knowledge and skills, and these may include additional new embedded check-on-learning, activities, and exercises. Refresher training will begin two (2) months after PSAP cutover and will leverage the same fixed and Mobile PSAP utilization approach presented in our Conversion and Administrator training approach. The refresher training materials will be included as a "Plug and Play" module as part of the Conversion Training Instructor Guide and Student Guide.

8.12.4. PSAP Administrator Training

The contractor shall present a plan to provide a four (4) hour comprehensive PSAP administrator training class. The contractor shall provide PSAP administrator training during implementation of any new sites or new equipment installations and as otherwise needed, with the assistance of State 911 Department as a resource as needed, and determined in the sole discretion of the State 911 Department. The contractor shall also be responsible for PSAP administrator training and certification of all State 911 Department Training and Systems staff, including training on any and all functionalities and/or payload types throughout the term of the contract and any renewal thereof.

Training shall include any and all site specific configuration/maintenance items to be performed by the PSAP administrator, as identified by the State 911 Department.

Training shall also include the operation and maintenance of management information systems supplied.

The scope of the PSAP Administrator course is to provide four hours of PSAP administrator and systems staff training. GDIT understands that this course needs to be delivered during the implementation of new sites, new equipment, or at the request of the State 911 Department. Following the same model presented in our Conversion Training overview, we will utilize the same ratio and class size planning for Administrator training. Assuming one (1) administrator position per-PSAP per shift, we estimate the staff quantity (average serving all PSAPs) to be approximately 714 total personnel. Following the same concurrent training model and leveraging the extra capacity available via our Conversion Training approach, the GDIT team will be able to use the same training schedule and locations for Administrator Training and the four (4) hour courses per session as required. Though the estimates provided in Conversion Training leave a 760 person-day availability, satisfying the 714 estimated staff herein, we recognize that the

actual numbers and disciplines will be different; the modeling provided here are to exhibit our collective planning and strategic model for delivering highly effective user training within the schedule requirements of this program. The curriculum for this training course will include the following:

- Functionalities and/or payload types
- Specific configuration/maintenance items to be performed by the PSAP administrator
- Operations and maintenance of management information systems supplied
- Site-specific configuration/maintenance items to be performed by the PSAP administrator

As with the Operations and Conversions Training requirements, we will apply our systematic development process to design and develop all the materials necessary to implement this four-hour certification program. Table 21 summarizes the proposed plan for the PSAP Administrator Training:

Table 21. PSAP Administrator Training Plan

Phase	Activities	Deliverable(s)
Analysis	• Conduct a thorough CFI analysis to confirm our understanding of the training and learning needs • Develop Course's Program of Instruction which includes the overall structure and sequence of the course including course description and learning objectives, topic outlines, list of lesson topics and modules with measurable objectives, course schedule, and assessment and evaluation strategies.	Course Program of Instruction Document
Design	The same templates that were approved by the State 911 Department for the Operations Training effort will be utilized	Course Materials Templates with Nomenclature Standards and Macros
Development	• Course content development for: – Course Instructor Administration Section – Lesson Plans – Teaching Aids (PowerPoint Slides) – Glossary – Practice Exercises Answer Keys – Test Package with Answer Keys • Student Guide – Course Student Administration Section – Glossary – Handouts – Practice Exercises	Draft Instructor Guides, Test Package, Practice Exercises Package, Student Guide with Exercises, and Handouts
Implementation	• Prepare train-the-trainer materials • Conduct train-the-trainer session with selected instructors	Train-the-trainer Materials Train-the-trainer After Session Report
Evaluation	• Final review to validate that training products meet GDIT's and the State 911 Department's standards and requirements for content validity and instructional soundness • Develop Course Materials Inventory • Conduct Pilot Testing (recommended)	Final Instructor Guides, Test Package, Practice Exercises Package, Student Guide with Exercises, and Handouts, Course Materials Inventory
Delivery	• Generate Gold Camera-ready copy for reproduction of course materials	Copies of Course Materials as needed.

Phase	Activities	Deliverable(s)
	• Ship copies of course materials to assigned locations	

As with the other two courses, similar course materials will be created that will yield to a comprehensive and instructionally sound Conversion Course using the "Plug and Play" approach.

8.12.5. State 911 Department Regional Training Centers

The contractor shall provide services to all State 911 Department regional training centers (currently four (4)). The current State 911 Department regional training centers are identified on Attachment K1- Primary PSAP, Regional PSAP, and RECC Data. The contractor shall install and maintain all equipment in each of the training centers for the duration of the contract and any renewals thereof. The contractor shall furnish the State 911 Department with updated training equipment and materials as needed.

Two (2) of the training centers shall have the capability to be a live working ten (10) position-training center capable of being used as a back-up PSAP and training center with the ability to simulate calls for training purposes. The State 911 Department reserves the right to move or add additional training centers.

Prior to the start of the conversion to the Next Generation 911 system, all training center shall have operational equipment with full functionality of that supplied to the PSAPs and capable of simulating calls, including payloads types.

The training center shall be designed and installed to allow State 911 Department trainers to train and certify newly hired enhanced 911 telecommunicators on the Next Generation 911 system and/or the legacy system during the conversion from the legacy system to the Next Generation 911 system.

The contractor shall be responsible for training the State 911 Department Training and Systems staff on the operations of each training center. The contractor is responsible for training State 911 Department staff if any new or upgraded CPE is added at those training centers.

Post conversion, the contractor shall be responsible for removing the legacy CPE at each training center, ensuring that the Next Generation 911 system is fully operational.

Prior to the start of the conversion to the NG9-1-1 system, GDIT will ensure that all training centers have operational equipment with full functionality of that supplied to the PSAPs, and that they are capable of simulating calls, including payloads types.

The training centers will be designed and installed to allow State 911 Department trainers to train and certify newly hired enhanced 9-1-1 telecommunicators on the NG9-1-1 system and/or the legacy system during the conversion from the legacy system to the NG9-1-1 system. Each training center will be designed to accommodate the optimum training atmosphere and environment, preparing the facility to have full operational functionality as provided to each PSAP. Training centers will be installed with the requisite hardware and software to conduct full-function NG9-1-1 call taker training, simulating call fluctuations, volumes, spikes, and payload types. Two of the regional training centers will be equipped with ten (10) positions and provisioned to be used not only for training but live answering of NG9-1-1 calls, serving as a backup or overload location.

GDIT will be responsible for training the State 911 Department Training and Systems staff on the operations of each training center, and will be responsible for training State 911 Department staff if any new or upgraded CPE is added at those training centers.

After conversion, GDIT will be responsible for removing the legacy CPE at each training center, ensuring that the NG9-1-1 system is fully operational.

All manpower and resources necessary to support all four State 911 Department regional training centers will be provided, to include equipment installation and maintenance, and updated training equipment and materials. Table 22 shows the summary of training tasks during each phase of the project.

Table 22. Training Tasks during Each Scheduled Phase

Scheduled Phase	Training
Pre-Implementation	New system equipment installation and updated training equipment and materials.
During Implementation	Train and certify newly hired enhanced 9-1-1 telecommunicators on the NG9-1-1 system and/or the legacy system Train the State 911 Department Training and Systems staff on the operations of each training center as well as any new or upgraded CPE added
Post-Implementation	Remove legacy CPE at each training center Ensure the NG9-1-1 system is fully operational.

8.12.6. Accessibility of Training

The contractor shall coordinate with the State 911 Department in the identification of all prospective attendees at its training who require accommodation, and shall cooperate with the State 911 Department in its provision of such accommodation.

All technical and user documentation and any additional training material delivered by the contractor under the contract, and any renewal thereof, shall include alternative keyboard commands that may be substituted for mouse commands, and shall, at the request of the State 911 Department, be provided in electronic format and/or printed in Braille.

GDIT has a long history of developing accessible training, or Section 508–compliant training for a variety of customers including various public safety clients: Defense Acquisition University (DAU); eArmyU; the Morale, Welfare, and Recreation Academy (MWR) of the U.S. Army; Veterans Health Administration (VHA); Veterans Benefits Administration (VBA); the U.S. Postal Service; and the Naval Education and Training Command (NETC).

Our involvement with Section 508 compliance began as early as 1999 when we were selected by the General Services Administration (GSA) and the Access Board to provide technical assistance to individuals and federal departments and agencies regarding the requirements of Section 508. To support this effort, GDIT developed instruction that is still available on U.S. government servers at: http://section508.gov under "508 Training." Since then, GDIT has developed Section 508–compliant training for a variety of modalities such as web-based training, instructor-led training, and electronic and paper documentation.

We will proactively coordinate with the State 911 Department to identify prospective attendees who may be hearing impaired, have visual disabilities at various degrees, or have psycho-motor disabilities. Alternate options will be provided as needed.

8.13. MIGRATION, DEPLOYMENT, AND INSTALLATION

As our core business, performance, and expertise are in providing mission-critical turn-key integrated systems for the DoD, we clearly understand the importance of the MA NG9-1-1 project. Even for the smallest PSAP in MA, failure of that PSAP can possibly cause serious public safety problems or even impair saving lives.

Keeping that in mind, our "Migration, Deployment, and Installation" approach will be based on "One Set of Goals" as shown in Figure 81.

Figure 81. GDIT MA NG9-1-1 Migration Goals

Our fully thought-out migration plan and associated activities will ensure we "do no harm" to the Commonwealth's emergency response capability. As it is one of the most critical objectives of the Commonwealth, GDIT's migration approach will be orchestrated in such a way that numerous forward-thinking parallel and advance preparation work will be done all along the schedule to ensure that we will meet the schedule requirements. Also, through our rigorous testing, verification, and validation processes, along with our up front approach with any issues or shortfalls, we will ensure that we deliver a reliable and functional system. Finally, as we have experienced with many previous large-scale complicated projects, it is very important that we collaborate with *all* stakeholders, to include service providers and operations personnel in the process.

Focusing on this "One Set of Goals," GDIT will ensure to perform and deliver the mission-critical MA NG9-1-1 system to the Commonwealth. In the following paragraphs, GDIT presents our phased migration and deployment strategy that fully aligns with the RFR specifications and project completion ahead of required 30 June 2016 completion date.

8.13.1. Migration Plan

Bidders shall factor the complete system installation into their response, including but not limited to, the stages identified below. Bidders shall complete the Project Schedule set forth in Attachment L- Project Schedule, Deliverables, and Milestones.

The system shall be fully operational throughout the Commonwealth no later than June 30, 2016. This deadline shall be strictly adhered to and shall be strictly enforced.

The Commonwealth's migration to Next Generation 911 will occur in a series of stages, operating in parallel, as follows:

A. System design and test plan development;

B. Laboratory trial and testing;

C. Data center installations, and pilot deployment at PSAPs to be selected and identified by the State 911 Department; and

D. Cutover on a rolling basis.

Bidders shall describe how they shall work cooperatively with the State 911 Department to finalize the migration plan, including without limitation, the following:

A. A detailed transition and migration and deployment plan for the delivery of calls from existing communication service providers to the Next Generation 911 system data centers. This plan shall accommodate communication service providers that continue to connect via the existing selective routers or directly to the data centers;

B. Participation in the transition and migration and deployment planning process and coordination with the existing carriers and for the ESInet;

C. How the bidder shall organize and support a rolling effort with respect to installation, provisioning, and testing;

D. How the bidder shall support the interconnection and integration of two disparate 911 systems – i.e., those working under Next Generation 911 parameters and those not yet cut over from the legacy system. Bidders shall describe in detail the process of transferring payloads from and to the existing selective routers during the transition period; and

E. Cutover planning and fall-back, if required.

The contractor shall submit a fallback plan that shall detail the roll back process.

GDIT will comply with the RFR specification.

Migrating the mission-critical E9-1-1 system with over 250 legacy PSAPs to the latest NG9-1-1 system is not for any team to take on; it is not just about technology, system, or products. This project requires a fully thought-out plan that is developed by highly experienced team. In particular, the migration plan must be methodically verified, tested, and re-validated before the actual implementation.

An essential element to success of the NG9-1-1 migration is experience on similar projects. GDIT has directly relevant depth and scope experience. GDIT engineered, implemented, and migrated the DoD's entire CONUS voice network – a migration effort required complex coordination with multiple agencies and hundreds of DoD installations. This project consisted of direct connections to 600 large-size PBXs with 1,700 T-1 circuits supporting 230,000 users. We successfully completed the project on time and on budget with A+ customer satisfaction.

Leveraging our extensive enterprise-level migration experience, GDIT will approach the NG9-1-1 migration in line with the Commonwealth's well thought-out phased migration framework as defined in the RFR. While embracing the framework, GDIT will further enhance the sequential and phased approach by orchestrating numerous forward-thinking parallel and advance preparation activities that will ensure not only that we fully test, verify, and prepare for the migration, but that our project schedule approach will also allow time to fix any unforeseen issues or problems in advance of the scheduled migration start date.

Figure 8 provides a high-level overview of our migration schedule approach on a phased and rolling basis.

GDIT's Migration Plan development won't occur over a few short weeks. Our multi-tied Migration Plan development approach and the effort will encompass the entire Milestone One through Three periods. We will develop a draft Migration Plan; collaborate with all stakeholders; update our plan based on lab testing; and further update it based on the data center and Pilot PSAP tests and cutover.

GDIT's migration plan development approach will start with assessment of current environment that will include but not limited to evaluating Commonwealth's data center(s), major PSAPs, network, facilities, and existing systems and infrastructures, such as selective routers and their locations. Additionally, we will review and discuss Commonwealth's current operations and associated polices to develop a draft migration plan framework. Upon developing a draft Migration Plan, the GDIT team will review and validate with all essential stakeholders, such as State 911 Department, EOPSS, carriers, and service providers to ensure all aspects of the migration is considered and validated. Our approach is illustrated in the Figure 82.

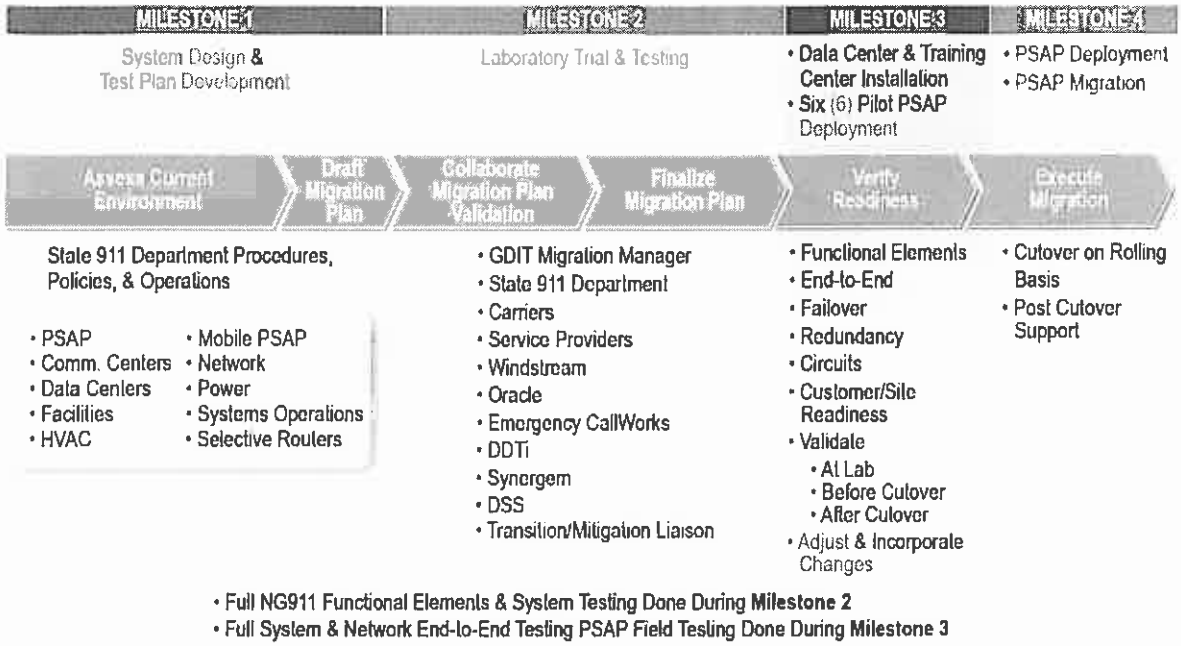


Figure 82. Migration Plan Development Approach

To ensure every critical aspects of the migration are considered, evaluated, and incorporated into the plan, it is necessary that we collaborate with all stakeholders throughout the migration process and as illustrated in Figure 83. During the collaboration process, we will adjust, incorporate essential inputs and processes, and also validate the plan.

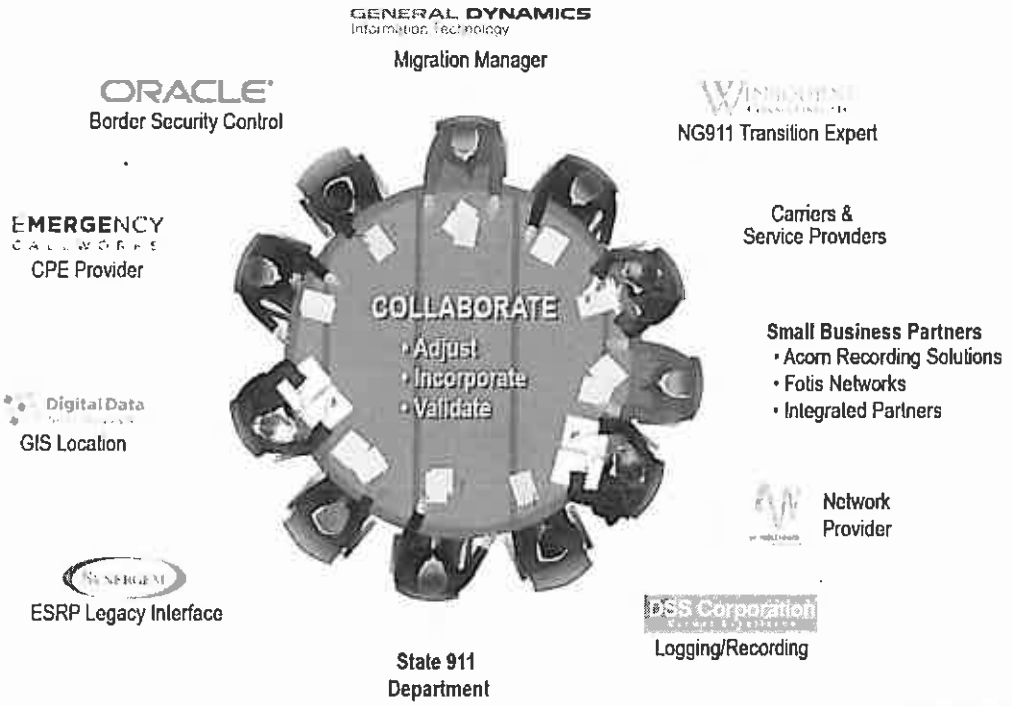


Figure 83. Migration Collaboration Team

Again, migrating to a new system is not just about technology, system, or products, but it requires a full cooperation and collaboration to develop a seamless and risk-mitigated plan for a successful migration. To orchestrate this, GDIT will be assigning a dedicated Migration Manager, who will be dedicated to developing the migration plan and also to direct the migration activities. The Migration Manager will be assisted by our team's NG9-1-1 Transition and Migration Advisor from Winbourne Consulting. Our Migration Manager will lead the effort to ensure the collaboration team brings to the forefront all vital migration-related issues and develops a fail-proof migration plan.

Section 8.7 (Next Generation 9-1-1 Architecture) provides technical details of migration and also collaboration necessary for this project.

While the Migration Manager is focused on developing the migration plan, our approach is that he/she must not worry about technical aspects of the NG9-1-1 system or the network. During Milestone 2 (Laboratory Trial and Testing), our Lab Manager will go through rigorous laboratory trials and testing of the NG9-1-1 system to ensure all functional elements are performing as required. Upon completion of the Milestone 3 (Data Center Installations and Pilot Deployment), our Migration Manager will further tweak the Milestone Plan based on the testing done during the phase. And, finally, during Milestone Phase 4 (PSAP Deployment), we will, for each and every PSAP, perform various pre- and post-cutover testing to again ensure we migrate the system as the Commonwealth expects.

Success-Oriented Migration Schedule

Our approach to a successful migration schedule is to start migration preparation well in advance to ensure we can mitigate any risk and be able to adapt to any unforeseen schedule delays. At the beginning of the Milestone 1, we will start the PSAP site survey with two dedicated teams, performing surveys and allowing them to complete all PSAP surveys by 6 April 2015.

For the Milestone 4 (PSAP Deployment) phase, we will have four dedicated PSAP implementation teams. Each team will perform site PSAP installation and testing, pre- and post-cutover testing and responsible for the site cutover. This PSAP migration approach will allow us to cutover all PSAPs by Week 93 (week of 8 May 2016) to include providing all required testing and acceptance documents.

Understanding that significant challenges could be posed in coordinating carriers and service-providers for transitions, as was shown in Figure 8, our Migration and Transition Plan development effort will require extensive coordination, collaboration, and agreement with the Commonwealth, carriers, and service providers. As our schedule shows, we will develop, validate, test, and re-validate the migration and transition methodology, sequences, and procedures, to include identifying all coordination points/contacts at each step of the migration prior to the actual PSAP deployment. Our Integrated Master Schedule (Appendix L) shows very details of every activities associated with PSAP migration.

GDIT will be teamed with Windstream Communications to support that coordination with the local service provider(s). Our dedicated Migration Management team will be responsible for circuit ordering and managing the process of implementation from circuit delivery to testing and activation/cutover. This team's specific focus will be the implementation scope of work, timelines, action items, and goals specifically related to making sure that the network circuits are available to support PSAP cutover schedules.

Utilizing the most proven, effective, and documented methods from order processing through cutover, test, and acceptance, Windstream's focus has always been on delivering a high quality of service from the beginning of the circuit ordering process, through the cutover and implementation of services, to the continuous day-to-day maintenance and support. This expertise in carrier transition and subsequent coordination has been integrated within GDIT's overall approach, a core competency that maximizes migration efficiency and minimizes risk, themes prevalent in GDIT's proposal and operational model.

Prior to installation, testing, and acceptance of each circuit at each site, GDIT and Windstream will coordinate with the Commonwealth for the approved cutover time in accordance with the project schedule based on a detailed cutover task list to ensure that there is no service impact on the Commonwealth and that the cutover is transparent to end users.

Circuits will be replaced one at a time, and the cutovers be scheduled for the PSAP's least busy time of day and day of week. Cutovers during normal business hours are encouraged in case escalations are required due to more resources and systems being generally available during these hours. The cutover plan will also detail the use of all commercially reasonable efforts to install services and perform the cutovers to the Windstream network from Verizon within the time frames set forth in the approved project schedule.

As part of the Migration Plan development effort, and in consultation with MassGIS, GDIT will develop and define the specific testing criteria necessary for effective and thorough GIS-centric testing. As call delivery in an NG9-1-1 environment is powered through geo-coordinates, ensuring the compatibility of services, functions, and processes herein is critical. The GDIT team of SMEs has direct and relevant experience in the field, which will greatly assist in defining the test cases and related functions necessary for this area. Working with State 911 Department and MassGIS, the GDIT team will develop and submit to State 911 Department the respective Test Cases, Scenarios, Reports for GIS Data, Database and LIS/LDB functions, Data Load Validation, Data Normalization and Load Testing as well as interrelated service dependencies with non-GIS specific functions. Deliverables to the State 911 Department that include Task Item 1.2.2 will include:

- GIS Data Test Plan
- Database, LIS, and LDB Test Plan
- Test Criteria
- Test Cases and Scenarios
- Test Reports

Critical to the success of this project is the availability and effective activation of the data centers, the hub of activity and location for NG9-1-1 services. While the test cases noted above will be used for these data centers at the subsystem and services level, the specific activation strategy and testing plan for data centers will be customized to the final design parameters and environment. GDIT will develop and submit to State 911 Department the requisite Data Center Test Plan which will include Test Criteria, Cases and Scenarios, and Test Reports for each data center. While the physical nature of each data center may differ (size, colocation of systems, HVAC, etc.), GDIT will approach both primary data centers as one unified system since they must function in unison to provide the required performance and redundancy.

Whereas each data center will receive its own test plan, the overall system will account for both locations and the performance requirements therein. Deliverables to State 911 Department during this effort for Task Item 1.2.3 will include:

- Data Center Test Plan
- Test Criteria
- Test Cases and Scenarios
- Test Reports (Independent and Paired)

Integral to the operational success of this project is provisioning a highly effective, robust, and intelligent Network Operations Center (NOC). GDIT has extensive experience in this arena, having developed and activated mission-critical NOCs around the world. We will use this expertise as we develop and submit to State 911 Department our NOC and Monitoring Test Plan, Cases, Scenarios, and Reports. GDIT will detail in this effort how our system will automatically generate trouble tickets, provide alarming and alerting functions to PSAP, staff, GDIT personnel, and the subsequently triaged deployment support entities and personnel. Deliverables to State 911 Department as part of this effort and in direct relation to Task Item 1.2.4 include:

- NOC Test Plan
- Monitoring Test Plan

- Test Cases and Test Scenarios
- Test Reports

One of the single most critical subject areas of any NG9-1-1 initiative is security, a domain that requires real-world expertise to ensure mission-critical system protection. This arena is another of GDIT's globally recognized realms of expertise, having secured some of the most threat-prone and sensitive environments in the world. This expertise will serve the Commonwealth now and into the future as more systems transition into the IP domain. Through GDIT's leadership in this field, adding future applications and network assets will be made possible through the rigorous security protocols and disciplines GDIT brings to this client-partnership. Our team will develop and submit to State 911 Department a detailed Security and Test Plan, along with the proven Test Criteria we have used in other mission-critical environments, delivering to the State 911 Department Task Item 1.2.5 elements, including:

- Security Test Plan
- Security Test Criteria
- Security Test Reports

Table 23 contains the summarized task items for Milestone 1 and proposed dates GDIT has prepared to align with the ultimate project date objective, as structured in the RFR.

Table 23. Milestone 1: System Design and Test Plan Development

Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
1.1	**System Design**		
1.1.1	Develop and Submit to the State 911 Department System Design and Technical Documents	Detailed System Design Documents	Within sixty (60) days of contract award
1.1.2	Develop and Submit to the State 911 Department Detailed Network Design and Technical Documents	Detailed Network Design and Technical Documents	Within sixty (60) days of contract award
1.1.3	Develop and Submit to the State 911 Department Data Center Assessment, System Design and Technical Documents	Data Center Assessment, System Design and Technical Documents	Within thirty (30) days of contract award
1.1.4	Develop and Submit to the State 911 Department Detailed Security Plan	Detailed Security Plan	Within sixty (60) days of contract award
1.1.5	Develop and Submit to the State 911 Department a NOC/Help Desk Operational Manual	NOC/Help Desk Operations Manual	Within sixty (60) days of contract award
1.2	**Test Plan Development**		
1.2.1	Develop and Submit to the State 911 Department System Test Plan, (including Network Test Plan), Test Criteria, Test Cases and Scenarios, and Test Reports for each functional element of the system	System Test Plan (including Network Test Plan), Test Criteria, Test Cases and Scenarios, and Test Reports	9/12/2014
1.2.2	Develop and Submit to the State 911 Department Test Plan, Test Criteria, Test Cases and Scenarios, and Test Reports for GIS Data, Database, and LIS server function, including initial data loading validation, data normalization and load	GIS Data, Database, and LIS Server Test Plan, Test Criteria, Test Cases and Scenarios, Test Reports	9/12/2014

Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
	testing		
1.2.3	Develop and Submit to the State 911 Department Data Center Test Plan, Test Criteria, Test Cases and Scenarios, and Test Reports, for each data center	Data Center Test Plan, Test Criteria, Test Cases and Scenarios, Test Reports for each data center	9/12/2014
1.2.4	Develop and Submit to the State 911 Department NOC and Monitoring Test Plan, Tests Cases and Scenarios, Test Reports, and document how the system automatically generates trouble tickets and alarming and alerting functions	NOC and Monitoring Test Plan, Test Criteria, Test Cases and Test Scenarios, Test Reports	9/12/2014
1.2.5	Develop and Submit to the State 911 Department Security Test Plan and Test Criteria	Security Test Plan and Security Test Criteria	9/12/2014
1.2.6	Develop and Submit to the State 911 Department Test Schedule	Test Schedule	9/12/2014
		MILESTONE DUE	**October 3, 2014**

To conclude this milestone section, GDIT will compile all of the preceding task plans and incorporate into a single, unified Test Schedule (Task Item 1.2.6), encapsulating all elements of the NG9-1-1 system and delivery process. This Master Schedule will be submitted to the State 911 Department and, upon acceptance and agreement by and between stakeholders, recognized as the official Test Schedule going forward. Assuming all dates and sequences align concurrent with the defined award date as currently noted, Milestone 1 will be completed by the targeted due date.

Milestone 2: Laboratory Trial and Testing

Upon formal acceptance of GDIT's Test Schedule, the team will commence with Milestone 2. In this stage, GDIT will establish the Laboratory Testing, Change Management Protocol, Software Release Testing and Deployment Strategy, Network Deployment Plans, Training Plan Development, and Pilot Cluster Deployment Documentation and Processes.

As described in "Milestone 1: System Design and Test Plan Development," GDIT will have already started the lab build-out and lab equipment installation. Utilizing this in-state NG9-1-1 lab and staging facility and having done the preliminary "leg-work" provides GDIT the unique ability to prepare with the State 911 Department well in advance of actual staging and deployments as well as post-cutover, ensuring that all applications and services conform to the testing parameters and operational requirements of the statewide solution.

During the Laboratory Trial and Testing Setup task, GDIT will establish the Staging and Trial Testing Plan specific to the Commonwealth's project objectives. The plan will be designed to minimize risk and maximize burn-in time in a non-production environment. The GDIT team and associated SMEs have a wealth of experience in NG9-1-1 systems development and field deployment of these technologies. With this expertise comes lessons-learned and knowledge of specific areas where additional and/or expanded testing will benefit all parties. This knowledge will contribute to our collective installation and configuration test strategy for applications, appliances, and CPE on simulated equipment in GDIT's NG9-1-1 staging and testing facility, our i3 Solutions Interoperability Lab.

Commensurate with this task area, GDIT will install and configure in its in-state lab the test equipment, applications, appliances, and CPE specific to this effort. Much of this has already been done by GDIT, having prepared the technologies and applications associated with GDIT's NG9-1-1 offering. These investments made in advance will greatly reduce deployment time and associated risks.

Deliverables to the State 911 Department for this task will include the following items as required in RFR Attachment L, Task Items 2.1.1 and 2.1.2:

- GDIT's Comprehensive Laboratory Staging Plan (Task 2.1.1)
- Trial Testing Plan
- Documentation on Test Equipment Readiness
- Documentation as to Application and Appliance Installation and Test Readiness
- Documentation as to CPE Installed and Preparation for Test Readiness

Once signoff is received for this set of tasks, the Laboratory Testing process will commence. During this phase GDIT will work with the State 911 Department Program Manager and assigned staff to fully exercise the NG9-1-1 solution in this simulated, yet highly realistic, lab environment.

As we enter this stage, a series of tasks and actions will be undertaken, following the protocols defined in Milestone 1 and applying them for testing of processes as well as applicability of these parameters. The first step will be to implement the System Test Plan for Milestone 1 items, exercising these elements until they have passed each test parameter. In conjunction with this and as the appliances and applications are so tightly integrated in NG9-1-1, GDIT will implement the GIS, Database, LIS/LDB and Server Test Plan in similar and parallel fashion. This will ensure that the LDB and database elements communicate with the ECRF, LVF, and ESRP services as designed. Any corrections and/or retesting will be performed as necessary until these elements are successfully passed.

Deliverables for this group of testing efforts will be commensurate with the elements defined in the RFR for Tasks 2.2.1 and 2.2.2 and will include:

- Final Test Results
- Application and Appliance Test Reports
- CPE Test Reports
- GIS, Database and LIS/LDB Test Results and Report

Separate from the applications and system testing, GDIT will develop and submit to State 911 Department its NSOC and Monitoring Test Plan, utilizing the simulated NG9-1-1 environment as the observation and resolution platform for testing purposes. Instrumental to this test effort will be the inclusion of GDIT's Security Test Plan, which will detail the intensive and systematic process that will simulate real-world operations and security threats to the system. Managing the deployed system is just as critical, if not more so, than the implementation of it, as operational security and system sustainability are crucial to the long-term success and Return on Investment (ROI). GDIT views these task areas as having the utmost importance, and we will work in partnership with State 911 Department and affected stakeholders to test any and all potential

intrusions, threats, operational scenarios, and catastrophic events to assure that system management and operational continuity are preserved.

Elements including event recording, quality of recording, network node visibility, layered access visibility, and payload monitoring are included in this effort. Final review and adjustment of documentation from the design phase will be performed to reflect the final post-test configuration. Deliverables to State 911 Department for Task Items 2.2.3 through 2.2.6 will include:

- NSOC and Monitoring Test Results and Report
- Updated Documentation
- Security Test Results
- Threat Analysis
- Event Recording Report
- Final Test Acceptance Documentation

To assure configuration rigidity and traceability, GDIT will develop and submit to the State 911 Department its Change Management Plan (detailed in Section 8.9.3, Change Management of this proposal) for hardware and software modifications, updates, software upgrade testing, and inventory updates. Included in this plan will be the process that will govern releases and the Change Management team that will ensure adherence to the process. Deliverables to the State 911 Department for Task Item 2.3.1 will include:

- Change Management Plan
- Software Release Management Plan
- Inventory Management Plan (to include Spares and Sparing Strategy)
- Documentation Updates

In accordance with Task Item 2.4, GDIT will commence with the finalization of Network Design and Deployment Plans, another section area that can potentially be run in parallel with the lab testing efforts to maximize time and schedule achievement. GDIT stresses the importance of testing and simulation and errs on the side of time invested up front as opposed to rushing to meet a schedule. While certain tasks can and will be run in parallel, our focus will be on maintaining overall solution quality and conformance, placing the required resources on subject areas holding the most critical elements (and risks) to the success of this project.

Tasks 2.4.1 and 2.4.2 will be undertaken and accomplished as GDIT prepares the final Network and Data Center Design and Deployment Plans, key milestones in the schedule which begin the transition and focus towards the field deployment phase. Included in this stage will be the revision and finalization of network design based on our thorough testing process results. This testing will assure that the deployed network is one that effectively provides the highest quality and reliability. Part and parcel to the network readiness is the finalization of Data Center Deployment Plans, accounting for the test results as well and including the staging strategy for Pilot PSAP deployment and order of subsequent clusters becoming final. Deliverables to State 911 Department for these Task Items will include:

- Final Network Design Document
- Final Data Center Design Document

- Final PSAP Deployment Plan

Upon formal approval of these preceding tasks, the GDIT team will focus efforts on developing and finalizing documentation packages that will be used for the Pilot PSAP deployment phase of the project. This documentation will serve as the baseline package for rollout to the PSAP community. Task Items 2.5 and 2.6 will be conducted by GDIT, integrating the training strategy with the Pilot cluster rollout and delivering to State 911 Department a highly detailed Training Plan for both Pilot PSAPs and State 911 Department staff. Deliverables for these Task Items will include:

- Training Plan
- Training Package/Materials
- Mobile Training Solution Documentation
- Pilot PSAP Deployment Training Schedule
- Pilot PSAP Deployment Plan
- Pilot PSAP Deployment Documentation
- Training Plan, Materials and Certification Training for State 911 Department Staff

Upon conclusion of these tasks, Milestone 2 will be met and GDIT will enter the deployment phase of the project. The highly regimented and tested processes and system elements will move the system closer to the production environment it was designed to serve. By undertaking this rigid testing process, GDIT is confident that the Pilot PSAP cluster deployment and data center installations will not only have potential risks mitigated, but it will allow for sequential phased installation of the remainder of the Commonwealth's PSAP clusters as detailed in the section for Milestone 4. As noted for Milestone 1, GDIT has designed its approach to include testing and leveraging advance planning and investments. Because of our approach, we will be able to meet the Milestone 2 completion due date as required.

Table 24 contains the summarized task items for Milestone 2 and proposed dates GDIT has prepared to align with the ultimate project date objective, as structured in the RFR:

Table 24. Milestone 2: Laboratory Trial and Testing

Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
2.1	**Laboratory Trial and Testing Setup**		
2.1.1	Establish Laboratory Staging and Trial Testing Plan	Comprehensive Laboratory Staging and Trial Testing Plan	9/7/2014
2.1.2	Install and Configure Test Equipment, Applications and Appliances and CPE using simulated equipment	Documentation that Test Equipment, Applications and Appliances, and CPE Installed and Prepared for Testing	9/22/2014
2.2	**Laboratory Testing**		
2.2.1	Implement System Test Plan and Correct/Retest as necessary until Test Passed	Final Test Results Report	10/6/2014
2.2.2	Implement GIS, Database, and LIS Server Test Plan and Correct/Retest as necessary until Test Passed	GIS, Database, and LIS Server Test Results Report	10/6/2014

Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
2.2.3	Implement NOC and Monitoring Test Plan and Correct/Retest as necessary until Test Passed and NOC processes and procedures refined to reflect results	NOC and Monitoring Test Results Report Updated Documentation	10/6/2014
2.2.4	Implement Security Test Plan	Security Test Results Report	10/6/2014
2.2.5	Event Recording Review and Refinement	Event Recording Results Report demonstrating operational functionality of Event Recording	10/7/2014
2.2.6	Lab Testing Review and adjust any documentation from design phase based on Lab Testing Results	Final Test Acceptance	10/7/2014
2.3	**Change Management Protocol Development**		
2.3.1	Develop and Submit to the State 911 Department Change Management Plan for hardware changes, software updates, software upgrade testing plan, determine change management team, inventory updates and documentation updates.	Change Management Plan	8/24/2014
2.4	**Finalize Network Design and Deployment Plans**		
2.4.1	Revise, Finalize, and Submit to the State 911 Department Network Design based on test results	Final Network Design Document	10/7/2014
2.4.2	Revise, Finalize, and Submit to the State 911 Department Data Center Deployment Plan, and PSAP Deployment Plan based on test results, Deployment Schedule for data centers and PSAPs submitted, planning complete, data centers prepared for commencement of pilot PSAP deployment, ordering schedule finalized	Final Data Center and PSAP Deployment Plan	11/5/2014
2.5	**Training Plan Development**		
2.5.1	Develop Training Plan and Training Materials working with State Department	Training Plan and Training Materials	9/12/2014
2.5.2	Develop Mobile Training Solution working with State 911 Department	Mobile Training Solution Documentation and Demonstration	10/7/2014
2.5.3	Develop PSAP Pilot Deployment Training Schedule working with State 911 Department	Pilot PSAP Deployment Training Schedule	11/1/2014
2.6	**Pilot Deployment Documentation and Processes**		
2.6.1	Develop and Submit to the State 911 Department Pilot PSAP Deployment Plan, Pilot PSAP Deployment Documentation (including Scheduling, Procurement, Installation, Quality Assurance and Work Order Documentation)	Pilot PSAP Deployment Plan and Pilot PSAP Deployment Documentation	10/27/2014

Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
2.6.2	In conjunction with State 911 Department, Develop and Deliver technical Training Plan and Materials to State 911 Department Systems staff and Develop and Deliver Training to State 911 Department Systems Staff on solution, read-only access to the Help Desk, and Monitoring systems	Training Plan and Materials and Certification of Training for State 911 Department Systems Staff	9/12/2014.
		MILESTONE DUE DATE	**December 3, 2014**

Milestone 3: Data Center Installations and Pilot Deployment

The milestone approach desired by the Commonwealth fits GDIT's transition strategy perfectly, as the deployment of data centers and the PSAP Pilot group provides a delivery point to safely benchmark the process. Working up to Milestone 3 requires an abundance of interaction and parallel coordination that spans Milestones 1, 2, and 3. In order to detail how the goals of Milestone 3 can be met, it is necessary to detail the entire physical process leading up to and through Milestone 3 to its completion.

Table 25. Milestone 3: Data Center Installations and Pilot Deployment

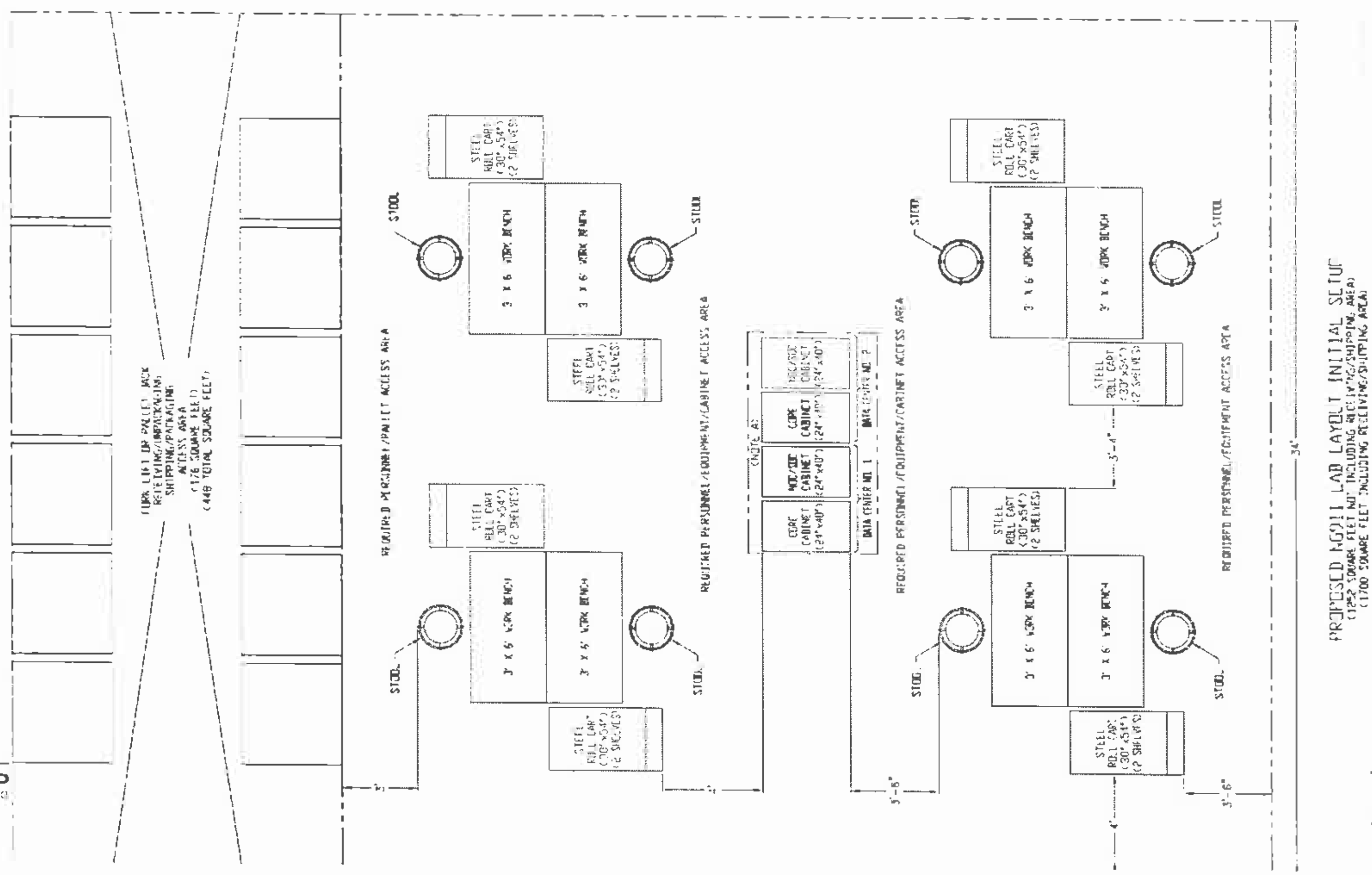
Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
3.1	**Data Center Installations**		
3.1.1	Install all equipment, applications, and appliances, and software at data centers for Pilot Deployment	Equipment, Applications and Appliances, and Software Installed in Data Centers	11/25/2014
3.1.2	Implement Data Center Test Plans (including Stress Test Plan, Data Center Failover Test, including routing failover, physical plant failover, security, application failover, routing, and call distribution	Test Results Reports for all Data Center Test Plans	12/1/2014
3.1.3	Working with the Executive Office of Public Safety and Security (EOPSS) and State 911 Department, develop Data Center Policies and Procedures for facilities, access procedures, security, notification and escalation processes	Data Center Policy and Procedures	11/24/2014
3.1.4	Review discussions, meetings and modifications as needed resulting from testing and data centers approved by the State 911 Department to be operational	Test Results, Acceptance Report, Site Acceptance Package for each Data Center	On or before Training Center Installation and PSAP Pilot Deployment 12/4/2014
3.2	**Training Center Installation**		
3.2.1	Install all equipment and CPE at Training Centers and connect Training Centers to Data Centers	State 911 Department Training Centers Operational Test Results, Acceptance Report, and Acceptance Package for each Training Center	On or before commencement of PSAP Pilot Deployment 1/28/2015
3.3	**PSAP Pilot Deployment**		
3.3.1	Prepare Six (6) Pilot PSAPs per PSAP	Site Cutover Project Plan,	11/26/2014

Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
	Pilot Deployment Plan approved by State 911 Department	Site Survey Form, Staging Test Results for each Pilot PSAP	
3.3.2	Cutover of Six (6) Pilot PSAPs in Pilot Deployment	Cutover Test Results, Post-Cutover Test Results, Cutover Acceptance Report, Site Cutover Acceptance Package for each Pilot Site	2/9/2015
		MILESTONE DUE DATE	**February 17, 2015**

Lab Staging

In conjunction with the ongoing design, procurement, and site survey efforts, preparations for laboratory trials and testing will be progressing. GDIT will employ a team of four engineers operating independently of each other and a dedicated logistician to work out of our Needham, MA facility. This team will begin receiving and assembling all the lab equipment, initializing, configuring, and conducting Pre-Installation Testing Check-Out (PITCO) beginning with the data centers, training centers, and the pilot PSAPs.

In a typical week, the engineer teams will each begin a PSAP system on Monday morning with an anticipated configuration and testing (PITCO) completion of 48 hours. Immediately following the completion of testing, each of the four PSAPs currently being staged will begin the 72-hour burn-in. While the current PSAP(s) are conducting burn-in, each engineer will then check out the next PSAP for configuration and test. This cycle will be maintained and potentially improved. GDIT's goal is to output approximately six PSAPs per month, a per-engineer effort equaling 24 field-ready PSAPs suites per month. The dedicated logistician will assist the engineering team in moving the systems to and from staging area and loading dock as well as keeping the systems tracked and maintained until the sites are scheduled and prepared for deployment/cutover. Figure 84 shows GDIT's i3 Solutions Interoperability Lab in Needham.



GENERAL D
Information Techn

Figure 84. GDIT I3 Solutions Interoperability Lab

All staging and testing requirements will be implemented. The security system testing with the NSOC will be set up and proven. Once all the functional areas have been tested, a 72-hour system burn-in will commence. After a successful burn-in, the functional acceptance report will be forwarded to the NG9-1-1 engineers for review. These steps will be followed for the data centers, all four training centers, six pilot PSAPs, and ultimately carry over to the remaining PSAPs to be built and deployed. Once these test evolutions are completed, these 12 systems can be de-installed from the lab and prepared for field deployment. GDIT will ensure system equipment arrives no sooner than 72 hours prior to installation. Final coordination is completed to ensure all the sites have been briefed and are ready for the impending installations. At this point Milestone 2 is complete.

Milestone 4: PSAP Deployment

As indicated earlier, GDIT will deploy four separate Field PSAP Implementation teams operating independently of each other at four different locations simultaneously to streamline productivity. The goal is for each team (nominally consisting of two engineers) to be onsite for approximately one week – yielding a cutover completion of approximately 16 sites per month. Cutover planning, submission, and approval will have been coordinated in preparation for the deployments in accordance with the RFR specifications.

From this point, each of the four site preparation teams will continue moving through the remaining PSAP clusters on a rolling basis in accordance with the approved schedule. Once equipment arrives, GDIT's four Field PSAP Teams will arrive as scheduled, conduct an in-brief, inventory and install all routers and switches, verify ESInet link integration, and test servers and GPS timing sources. All cabling will be pulled, terminated, and labeled. Once the site is powered up, final configurations will be performed. The deployments will begin with both data centers and progress through all four training centers (Maynard 10, Maynard 13, Taunton, and Springfield). Prior to deployment of the first PSAP, training will have to be coordinated for all individuals affected by the first six pilot PSAP installations. At each location, once servers are installed, we will place all the call taker position workstations and accessories. Once training has been completed and approved, the six pilot PSAPs will follow. At this point, Milestone #3 is complete.

Guided by the Integrated Master Schedule (IMS), the four distinct Lab and Fielding Teams will be staging, testing, deploying, and cutting over PSAPs. The installation plan for the remainder of the PSAPs will be facilitated by the fact that the site preparation and ESInet link will have already been completed. The final milestone, staging and deployment of the eight PSAP groups, will be conducted over a period of approximately 1.5 years following the data centers, training centers and pilot PSAPs. By Week 93 (first week of May 2016), GDIT plans to complete all PSAP cutovers. This schedule approach provides yet another buffer to account for and recover from any unexpected issues until end of June 2016. As each PSAP is deemed "fit for service," the existing 9-1-1 systems will be decommissioned. GDIT will coordinate with the State 911 Department for removal and final disposition of legacy equipment.

As carrier redundancy and legacy system sustainability through cutover are critical elements to the sequential transition to this NG9-1-1 environment, the GDIT team is aligning its migration to best activate the respective physical core networks (by carrier) and the respective PSAP clusters each carrier serves. Leveraging the state-provided network assets, we have a dual-path, triply-

redundant cluster model that allows for PSAP activation, site cutover, PSAP cluster activation and trunk transition, and carrier-backbone specific network migration serving the cluster. Trunks will be transitioned from the respective carriers to the data centers as the final step in this process for each of the clusters, allowing for parallel burn-in and throughput testing of each NG9-1-1 region while maintaining the legacy 9-1-1 system. To test all facets of the NG9-1-1 solution, GDIT looks at each of these core networks as a logical network group – each one comprising the master ESInet solution upon statewide deployment and cutover.

As each regional group aligns with the secondary and tertiary assets of the MassNet vision, our model allows for cutover not only of the PSAPs and clusters of each, but uses the secondary network as the means of transition prior to cutting the primary carrier trunks. For example, the PSAPs that have connectivity to the Mass 1,2,3 assets managed by Axia Networks would first be provisioned and tested on those network assets with connectivity to the legacy 9-1-1 system maintained from the Selective Router (with LNG colocation providing connectivity to legacy system to NG9-1-1 PSAPs rather than burdening the cost of LPGs unnecessarily) to the PSAPs directly.

Upon acceptance of the site and Axia-provided network services, calls from the carrier will be repointed to aggregate at the data centers while the cluster runs in parallel for the minimum 30-day burn-in period, during which time the carrier data circuits to each PSAP are provisioned. Repeating the steps of cutting onto the Axia-provided network, the carrier-core assets will undergo the same burn-in – a bottoms-up approach to readying the PSAP and cluster for logical network connectivity to the ESInet. As each regional cluster is cutover and primary and secondary access provisioned, that cluster is connected to the ESInet with ingress and egress transitioning through the data centers.

Utilizing the secondary assets affords many advantages in addition to risk mitigation, as one of the most complex challenges that this type of project presents is facilitating the carrier transition. Carrier transition does not allow for a flash cutover or traditional site cutover approach. Rather than install temporary trunks to each PSAP, GDIT has designed its migration as a large systems integrator must, assessing all elements involved in the call flow today, the network architecture proposed, and the carrier services to each required.

Upon acceptance of the logical network cluster (the NG9-1-1 ring of PSAPs aligned with the MassNet physical regions and assets), legacy 9-1-1 circuits to each PSAP will be decommissioned and re-pointed from the selective router to the data centers. As each regional cluster is successfully cutover and accepted according to the above example, the ESInet grows and becomes inherently more redundant. As more diverse physical core network assets build up the logical ESInet environment, redundancy and failover options emerge which are far superior to the legacy 9-1-1 network limitations today.

For Milestones 4.1 through 4.8, GDIT will be able to effectively achieve the required dates in this model while affording the Commonwealth the phased burn-in and cutover process necessary for this level of integration effort. With respect to the larger PSAPs, GDIT recommends specifically detailing with their team (in accordance with Milestone 1) specific trunk and route options that will best serve their unique environments, call flows, traffic volumes, and diversity requirements. GDIT recognizes that a one-size-fits-all solution will not prevail. Our design and migration strategy to transition to the NG9-1-1 environment allows us to meet the statewide

objectives and, as we work as the Commonwealth's technology integration and service partner, define and customize the network and provisioning to serve their respective metro-area needs best.

By completion of the project, GDIT will have led this migration as the change agent for the Commonwealth. Together, we will have successfully provisioned the largest, most diverse NG9-1-1 solution in the nation – an achievement that can only be accomplished by focusing on rigorous risk mitigation and attending to all details as noted above and throughout our proposal. This level of discipline and project control is what GDIT is known for and why the world's most mission-critical operations trust in our services. We intend to earn this same trust and confidence from the Commonwealth's NG9-1-1 team and agency stakeholders.

Table 26 contains the summarized task items for Milestone 4 and the dates GDIT proposes to align with the ultimate project date objectives. Our schedule accounts for the clustering and cutover strategy recommended for this project and is based on the sequential approach to PSAP implementation.

Table 26. Milestone 4: PSAP Deployment*

Deliverable/ Task Number	Deliverable/ Task Name	Deliverable(s)	Deliverable Due Date
4.1	Cutover of 20 PSAPs	Cutover Acceptance Report for 20 PSAPs	April 30, 2015
4.2	Cutover of 30 PSAPs	Cutover Acceptance Report for 30 PSAPs	June 30, 2015
4.3	Cutover of 34 PSAPs	Cutover Acceptance Report for 34 PSAPs	August 31, 2015
4.4	Cutover of 34 PSAPs	Cutover Acceptance Report for 34 PSAPs	October 31, 2015
4.5	Cutover of 28 PSAPs	Cutover Acceptance Report for 28 PSAPs	December 31, 2015
4.6	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	February 28, 2016
4.7	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	April 30, 2016
4.8	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	June 30, 2016
		MILESTONE DUE DATE	**June 30, 2016**

** Note: This milestone includes the Mobile PSAP and from Attachment G – Boston Fire, Springfield Fire, and Worcester Fire*

8.13.2. System Installation

GDIT will comply with the RFR specification.

Commensurate with the detailed Project Plan that will be developed as discussed in Section 8.9 (Project Management), GDIT will follow a disciplined methodology, segmenting installation activities into two phases. GDIT proposes utilization of its highly regimented and subcontractor-recognized program approach and methodology for the MA NG9-1-1 project. Following this phased model allows all stakeholders to benefit from a solution-driven focus through the discipline of a large systems integrator's Quality Management Program (QMP) approach.

Our detailed approach not only conforms to the Commonwealths' CommonWay system, but it aligns with the subcontractors GDIT has assembled for this initiative and their respective core competencies and areas of subject matter expertise. While our in-state PMP-certified Project Manager will provide overall project leadership and oversight, the respective Project Managers from each subcontractor will be responsible for task and action item ownership for their areas of technology and/or solution provisioning. Working in concert with these industry-proven experts

in their respective core competencies, the GDIT Project Manager will have a team of professionals not only committed to this project for the duration, but who hold decades of 9-1-1 industry experience that bolsters our team's collective resume and expertise in leadership.

Field installation activities will be conducted by a strike team of core-competency technology leads from the NG9-1-1 solution providers, led by the GDIT Project Manager and Field Implementation Manager. As detailed in Section 8.13.1 (Migration Plan), our team will follow the approach of Milestones 3 and 4 and, in clusters, install on a rolling basis the PSAP clusters defined under Milestone 4.

The field implementation team will install the solution as designed with configuration instructions as developed during Milestone phases 1 and 2 as noted in Section 8.13.1.

Immediately following contract award, our team will focus on Milestone #1: the System Design and Test Plan Development. A majority of this work has been performed during the solicitation phase. A team of engineers will finalize the System Design and Test Plan.

GDIT will then begin a 40-day procurement phase. Utilizing the detailed BOM that we have already developed, our process can be prioritized to focus on lab equipment. Also in the first month, a Project Kickoff Meeting will convene. Highlights of this meeting will include the site survey schedule and site preparations to be conducted in advance of the data centers, training centers, and PSAP deployments.

As stated previously, we plan to use two separate site survey teams. Once the training centers and pilot PSAPs are surveyed, we will submit reports to begin the MA NG9-1-1 review/approval cycle. Our normal PSAP surveys will continue in eight successive groups for the next eight months. Our priorities will be developed with NG9-1-1 officials and clearly linked to the migration plan.

This scheduling will allow one of our key installation strategies to emerge: once a PSAP survey is finished and approved, and coordination with each site is done, a PSAP site preparation BOM will be created and the site preparation team can be dispatched to that site. Once survey approvals are received, GDIT will develop site drawings. GDIT will deploy four separate site preparation teams. For a small PSAP, each team will nominally consist of two technicians who will be on site for one week. We want the site preparation team to be "independent" of the fielding team to streamline productivity. Once the cabinets, electrical work, GPS timing sources, and cabling are all installed and inspected, that site is ready for the fielding team.

Our site preparation will begin with both data centers and progress through all four training centers (Maynard 10, Maynard 13, Taunton, and Springfield). The six pilot PSAPs, once designated by State 911 Department and GDIT, will follow. Then the eight groups of between 20 and 35 PSAP sites will be prepared. All site preparation work is scheduled to be completed in early 2016. The large position count PSAPs will have special planning and teams to support the additional planning and effort required.

In conjunction with the final design, procurement, and site surveys, Laboratory Trials and Testing will be progressing. Our team of four engineers and technicians will work at our Needham, MA facility. This team will assemble all the equipment, perform initializations and configurations, and conduct Pre-Installation Testing Check-Out (PITCO). All ESInet testing

requirements will be implemented. The security system testing with the Network and Security Operations Center (NSOC) will be set up and proven. Once all the functional areas have been tested, a 72-hour system burn-in will commence. After a successful burn-in, the functional acceptance report will be forwarded to the NG9-1-1 engineers for review. These steps will be followed for both data centers, all four training centers and the six (6) pilot PSAPs. This is Milestone #2.

Once these test evolutions are completed, these 12 systems can be de-installed from the lab and prepared for field deployment. GDIT will ensure system equipment arrives no sooner than 72 hours prior to installation. Final coordination is completed to ensure all the sites have been briefed and are ready for the impending installations.

Once the equipment is on site, GDIT's four Fielding Teams will arrive as scheduled, conduct an in-brief, and inventory and install all routers, switches, servers, and GPS timing sources. All cabling will be pulled, terminated, and labeled. Once the site is powered up, final configurations will be performed. The chronology for this evolution is Data Center 1 and Data Center 2 will be installed. Then, all four training sites will be undertaken simultaneously. At each location, once servers are installed, we will place all the call taker position workstations and accessories. The next step is to verify ESInet integration and testing. GDIT will conduct this testing with our ECW partners.

After the successful testing of data centers and training sites, we move into the initial cutover phase. Cutover planning, submission, and approval have been completed (including pilot PSAP Cutover Plans).

We will then cutover the four training centers followed by the six pilot PSAPs with dates and times coordinated. At this point, Milestone #3 is complete.

The installation plan for the majority of the small PSAPs will be facilitated by the fact that the site preparation work has been completed. In the GDIT i3 Solutions Interoperability Lab, a typical week will involve four engineers/technicians each beginning a PSAP system on Monday morning. By Thursday, each of the four systems will begin the 72-hour burn-in. Each technician will begin setting up, configuring, and testing (PITCO) another set of gear. This cycle will be maintained and potentially improved. Our plan is to produce 24 field-ready PSAPs suites per month. A dedicated logistician will assist the technical team moving the systems to and from the loading dock.

GDIT develop a rhythm of surveys, deliverable document submittals, site preparation, PSAP suite deliveries, and field installations. The final milestone, the staging and deployment of the eight groups of small PSAPs, will be conducted over a period of approximately one year. Guided by our Plan of Action and Milestones (POA&M), our four distinct Lab and Fielding Teams will be building, testing, and cutting over PSAPs.

Upon PSAP migration acceptance (deemed "fit for service"), currently existing systems will be decommissioned. Removal and storage/disposition of legacy equipment will be ascertained by State 911 Department.

8.13.2.1. Quality Assurance Requirements

The contractor shall design and establish a quality control system and procedures to ensure that hardware and software supplies and/or services meet the quality standards specified in this RFR. The quality control system, including procedures, shall be subject to the prior approval of the Department and shall also be subject to inspection by the State 911 Department. Adherence to the quality control sub-specification and any procedure or document in implementation thereof shall not release the contractor from any other requirements of the contract.

The quality control system shall ensure that adequate control of quality is maintained throughout all areas of contract performance, including without limitation, the receipt, identification, stocking, and issuance of material, the entire physical process of manufacture, packaging, shipping, storage, installation, and maintenance, and processes of software development, design structure, coding, testing, integration, and implementation.

All equipment, supplies, and services provided under the contract, whether manufactured or performed at the contractor's facility or at any other source, shall be subject to control at such points as necessary to ensure conformity with the specifications and contractual requirements. The system shall provide for the prevention and ready detection of discrepancies and for timely and positive corrective action. The contractor shall provide objective evidence of quality performance to the State 911 Department upon request.

GDIT complies with the RFR specification.

ISO 9001 certifications, adherence to industry-accepted standards for quality and performance, and compliance with our Quality Management System (QMS) and Quality Environmental Health and Safety System (QEHS) positively affect the way GDIT does business. ISO 9001:2008 standardizes the processes and procedures we use. Simply put, we plan what we do, do what we say, measure how well we do, and act based on the results of audits, quality control inspections, validations, and evaluations. This process ensures that the State 911 Department will receive the highest quality hardware and software supplies and services explicitly and implicitly specified in the RFR from the GDIT team. Every corporate element supporting the GDIT team works within our QEHS processes and procedures; this includes our teammates, partners, and other subcontractors. For those teammates who are not ISO 9001 certified, GDIT will provide mentorship to help them understand the importance of ISO 9001, our QEHS, and quality performance. This ensures that our teammates are aligned with our quality goals, which are driven by our customer's requirements.

Our ISO 9001 certification by SAI Global means that we are certified for contract performance to include the engineering, design, development, fabrication, testing, installation, operation, maintenance, training, and support systems for information technology/communications systems and networks and military applications worldwide. This also includes the design and manufacture of related equipment. GDIT uses the ISO 9001:2008, ISO 14001:2004, and OHSAS 18001:2007 standards as an overall model for our QMS, and supplements those standards with other models, methods, and tools, including the Capability Maturity Model Integration (CMMI), which is key in software development; IT Infrastructure Library (ITIL); Earned Value Management System (EVMS); and Lean Six Sigma (LSS), etc., as appropriate to meet GDIT's business requirements.

Quality Control Plan

A draft Quality Control Plan (QCP) will be provided and briefed after award for review. GDIT will devise new procedures, as necessary, to meet the explicit approval of the State 911 Department. The QCP will establish a benchmark for effective development of quality control procedures and will ensure that GDIT has implemented quality control effectively across all requirements of this project. The quality process will be closely aligned with the project's testing

strategies and processes. Our internal quality control program will establish tracking records for all measurable performance requirements listed within this contract. GDIT will incorporate the following minimum elements into the QCP:

- Definition of contractor quality-control-management lines of responsibility
- Quality Control Management System Process
- Quality Standards
- Internal Design Review/Change Control Process
- Internal Document Control Process
- Process for preliminary systems testing and validation
- Process for the execution of corrective actions
- Process for maintaining quality assurance records throughout the project life cycle
- Process for performing random internal quality control audits

Preventative and Corrective Actions

GDIT has established procedures to identify actual/potential defects, nonconformities, and methods for improvements in our processes and to correct and prevent future recurrence. These procedures provide a mechanism for reporting, documenting, and managing current and potential problems that adversely affect quality to ensure rapid and effective resolution.

Preventive action includes the review and analysis of all information sources to detect and eliminate potential problems in procedures or processes. "Lessons learned" are collected at various stages throughout a program or project's life cycle and are evaluated to determine what changes are to be made in an effort to achieve continual improvement.

- GDIT's preventive action process requires:
- Determining potential nonconformities and their causes
- Evaluating the need for action to prevent occurrences of nonconformities
- Determining and implementing action(s) needed
- Records of results of action taken
- Reviewing preventive action taken and determination of continual improvement opportunities

The GDIT team collects "lessons learned" at various stages throughout a program or project's life cycle, and these are evaluated to determine what changes are to be made in an effort to achieve continual improvement.

GDIT's QMS, through implementation of a QCP approved by the State and backed by our ISO 9001 certifications and proven methods for preventing and correcting deficiencies, will ensure that quality control is maintained throughout all areas of contract performance, including, as applicable, the receipt, identification, stocking, and issuance of material; the entire physical process of manufacturing, packaging, shipping, storage, installation, and maintenance; and software development processes, including design structure, coding, testing, integration, and implementation.

8.13.3. System Testing

The contractor shall develop and shall submit to the State 911 Department for approval a comprehensive test plan for the system, for each functional element of the system, the network, and for each PSAP, that addresses, at a minimum, the following test procedures. The contractor shall apply the following acceptance test procedures to the individual systems as they are installed and prior to any live operation. The contractor shall also apply test procedures to the system prior to providing final system acceptance.

The comprehensive test plan shall address, at a minimum, the proposed test environment, test facility, test equipment, test configuration, test thresholds, test call simulators, and test documentation. The contractor shall conduct all system testing at an i3-compatible laboratory approved by the State 911 Department, and the State 911 Department reserves the right to require testing at the State 911 Department's facilities and/or training centers. The contractor shall provide to the State 911 Department for its approval documentation that demonstrates that the applications, appliances, and CPE for the system are ready for testing. The State 911 Department reserves the right to inspect the test equipment, applications and appliances, and CPE have been properly configured and installed. The contractor shall refine and resubmit the system design and technical documents to reflect results of system testing.

GDIT will comply with the RFR specification.

GDIT will develop, and submit to the State 911 Department for approval, complete Acceptance Test Plans for each data center functional element, ESInet, and for each PSAP. The Acceptance Test Plans will be based on the manufacturer's best commercial practices, industry standards, and recommendations provided by the State 911 Department to test/verify/inspect all systems delivered. Each Acceptance Test Plan will contain:

- Listing of applicable reference documents and points of contact for the testing program
- Technical description for the system under test
- Test schedule
- Identification of test and measurement equipment to be used
- Test procedures with expected test results that define a passing test
- Appendix to document discrepancies
- Appendix for Acceptance Test sign-off

As shown in Table 27, GDIT will develop extensive test cases and scenarios for each component of the system, NG9-1-1 functional elements, system, ESInet, and end-to-end testing and failover cases. Each test plan will be re-validated, re-tested, and updated again to ensure all aspects of the system are solid for migration.

Table 27. System Test Plan Development and Testing Approach

Milestone 1	Milestone 2	Milestone 3	Milestone 4
System Design and Test Plan Development	**Laboratory Trial and Testing**	**Data Center Installations and Pilot Deployment**	**PSAP Deployment**
• Develop Comprehensive Test Plan • Test Cases • Scenarios • Reports • System • Network • Network Management • NSOC • System Failovers • DC Failovers • Traffic Routing • Failback • ESInet Test Procedures • NG9-1-1 Functional Test • **Needham MA i3 Solutions Interoperability Lab State Approval for I3 Compatibility**	• At GDIT MA NG9-1-1 Needham, MA Lab Test Plan Exercised Test Plan Updated	• At Data Centers and Pilot PSAPs • Test Plan Implemented • Test Plan Updated • Pilot PSAP Test • PSAP Pre- & Post-Cutover Test Plan • Updated	• Pre- & Post-Cutover Functional Tests • Test Cases • Scenarios • Reports

All tests performed during the staging process will be conducted at an i3-compatible laboratory approved by the State 911 Department. GDIT intends to use its facility in Needham, Massachusetts for staging. GDIT understands that the State 911 Department reserves the right to require the testing at the State 911 Department's facilities or training centers. GDIT will provide documentation to the State 911 Department that demonstrates that the staged equipment is ready for testing. GDIT understands that the State 911 Department may choose to inspect test equipment, applications/appliances, and CPE for proper installation and configuration. GDIT will update and resubmit system design/technical documentation to reflect the results of system testing.

8.13.3.1. ESInet Test Procedure

The contractor shall design, conduct, pass, and document a thorough test procedure for the network and network monitoring components of the system. This test plan shall at minimum, confirm that these components meet the specifications in the RFR as well as any other requirements necessary for the compliance with applicable standards, rules, and regulations.

This shall include, but not be limited to, tests for:

- *Data Center end-to-end connectivity of all circuits;*
- *Throughput;*
- *Packet loss;*
- *Latency;*
- *Jitter;*
- *Routing;*
- *QoS mechanisms;*
- *Fault recovery;*

- *Fail-over from primary to secondary paths;*
- *Simulation of peak traffic load for a minimum of twenty-four (24) hours;*
- *Network monitoring systems;*
- *Faulty notification systems;*
- *Firewalls, intrusion detection systems, intrusion protection systems; and*
- *Data Center network connections to third parties (LEC's, Internet, etc.)*

GDIT will comply with the RFR specification.

An example of initial Acceptance Test Procedure (ATP) is shown below for demonstrating network reliability in compliance with system design and requirements. Fourteen (14) scenarios are included below, for example purposes only, although each scenario will likely be demonstrated as independent tests on separate forms. Each ATP template will be modified to include specific steps for each scenario and subsystem installation and will be subject to the approval of the State 911 Department.

Test Item Number	**Test Title**	**SRD Reference**	**Test Type**
1	ESInet	8.13.3.1	Demonstration

Contract Name	**Contract Number**
MA NG9-1-1	TBD (template/example data only)

State 911 Department Support / Windstream Support – May be required
Template/example data only – GDIT engineers to identify and detail actual steps for each subsystem

Requirement(s) (template/example data only)
The following test can be performed from the following location: xxx
The following quantity of systems and software will be used to perform the test:

- (1) ESInet workstation, connected to the ESInet management network, running the xxx application
- (1) Network applications/tools in customer environment (list specific tools when available)

Required Test Data
The following account information needs to be obtained:

- ESInet\ESInet_Admins member AD account and password
- Applicable service account and password (list specific service account when available)

Test Scenario (template/example data only)
Connect to the Network Node using customer approved tools (list when identified). Open the application on the ESInet workstation. Verify that all screens and reports are functional and displaying valid data within the expected parameters for each scenario:
Test 1.1 – End-to-End Connectivity of All Data Center Circuits
Test 1.2 – Throughput
Test 1.3 – Packet Loss
Test 1.4 – Latency
Test 1.5 – Jitter
Test 1.6 – Routing
Test 1.7 – Quality of Service (QoS) Mechanisms
Test 1.8 – Fault Recovery
Test 1.9 – Fail-over from Primary to Secondary Paths
Test 1.10 – Simulate 200% of Peak Traffic for 24 hours

Test 1.11 – Network Monitoring Systems
Test 1.12 – Fault Notification Systems
Test 1.13.1 – Firewalls
Test 1.13.2 – Intrusion Detection Systems
Test 1.13.3 – Intrusion Protection Systems
Test 1.14 – Data Center Network Connections to Third Parties (LECs, Internet, etc.)

Unusual Requirements/Risks	**Support Equipment Identification**
As needed	**Software Version:** List when identified **Platform:**

Procedures (template/example data only)

Test 1.1 – End-to-End Connectivity of All Data Center Circuits:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.2 – Throughput:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
4. Perform step 4
5. Exit

Test 1.3 – Packet Loss:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.4 – Latency:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 4
3. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test

4. Exit

Test 1.5 – Jitter:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
5. Exit

Test 1.6 – Routing:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.7 – Quality of Service (QoS) Mechanisms:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
4. Perform step 4
5. Exit

Test 1.8 – Fault Recovery:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.9 – Fail-over from Primary to Secondary Paths:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command

used to execute code
needed to complete test

6. Exit

Test 1.10 – Simulate 200% of Peak Traffic for 24-hours:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.11 – Network Monitoring Systems:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.12 – Fault Notification Systems:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.13.1 – Firewalls:

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)
2. Perform step 2
3. etc.

Test 1.13.2 – Intrusion Detection Systems:

1. Log into xxx using the xxx-adm account.
2. etc.

Test 1.13.3 – Intrusion Protection Systems:

1. Log into xxx using the xxx-adm account.
2. etc.

Test 1.14 – Data Center Network Connections to Third Parties (LECs, Internet, etc.):

1. Log into xxx using the xxx-adm account. (Network Engineer to develop specific technical steps)

2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Expected Results

Test 1.1: Expected results…All circuits communicating….
Test 1.2: Record Expected Results
Test 1.3: Monthly average packet loss between demarcation points not to exceed 0.5%
Test 1.4: Packet Latency an average round trip time of 40ms (equates to 1-way transmission time of 20 ms)
Test 1.5: Jitter shall not exceed twenty (20) milliseconds
Test 1.6: Verify network packets and/or test calls route as required
Test 1.7: Record QoS expectations…
Test 1.8: Fault Recovery Expectations
Test 1.9: Failover from Primary to Secondary paths works consistently as expected, on demand
Test 1.10: No test/traffic system or subsystem failures while simulating 200% of peak traffic for 24-hours
Test 1.11: Network Monitoring Systems…
Test 1.12: Fault notifications sent to identify…
Test 1.13.1: Firewalls: Detail Expected Results
Test 1.13.2: Intrusion Detection Systems: Detail Expected Results
Test 1.13.3: Intrusion Protection Systems: Detail Expected Results
Test 1.14: Record Expected Results

Actual Results

Test 1.1: Actual Results….All circuits communicating…
Test 1.2: Record Actual Results
Test 1.3: Monthly average packet loss between demarcation points not to exceed 0.5%
Test 1.4: Packet Latency average round trip time of 40ms (equates to 1-way transmission time of 20 ms)
Test 1.5: Jitter shall not exceed twenty (20) milliseconds
Test 1.6: Verify network packets and/or test calls route as required
Test 1.7: Record QoS expectations…
Test 1.8: Fault Recovery Expectations
Test 1.9: Failover from Primary to Secondary paths works consistently as expected, on demand
Test 1.10: No test/traffic system or subsystem failures while simulating 200% of peak traffic for 24-hours
Test 1.11: Network Monitoring Systems…
Test 1.12: Fault notifications sent to identify…
Test 1.13.1: Firewalls: Detail Expected Results
Test 1.13.2: Intrusion Detection Systems: Detail Expected Results
Test 1.13.3: Intrusion Protection Systems: Detail Expected Results
Test 1.14: Record Expected Results

Comments/Additional Findings

Test Results (Pass/Fail)	**Verified By:**

☐ Pass ☐ Fail	GDIT Engineer: _____ Name Initials Date Customer Sysadmin: _____ Name Initials Date

8.13.3.2. Functional Acceptance Test

The contractor shall conduct a functional acceptance test to verify that the systems installed provide the expected functional capabilities in accordance with the design criteria for the system. The contractor shall demonstrate to the satisfaction of the State 911 Department that each function and option operates according to the design documentation, including the RFR, and applicable standards. Shall any failures be identified during the test, the contractor will have a reasonable opportunity to correct the deficiencies, after which a retest may be scheduled. The State 911 Department, at its sole discretion, may require a retest of the failed functions, or may elect to require the contractor to conduct a complete retest. This process will continue until all functions have passed or it becomes obvious that the system under test will not support one or more functions that it was designed to accomplish. At this point, the State 911 Department may negotiate a settlement with the contractor, or may take other steps as deemed appropriate.

Proposals shall include a proposed initial acceptance test plan (ATP) for demonstrating the system functions. The ATP shall be subject to the approval of the State 911 Department.

A proposed initial Acceptance Test Plan (ATP) for the Functional Acceptance Test is shown below. This Functional Acceptance Test ATP defines the test plan and records test results. The ATP template will be modified to include specific steps for each subsystem installation and will be subject to the approval of the State 911 Department.

GDIT will comply with the RFR specification. The example Acceptance Test Plan (ATP) below includes 11 scenarios, all tested with DDTi ECRF/LVR 1.0 software to demonstrate the functionality of ECRF/LVR systems. These example scenarios are consolidated into one ATP for example purposes only. Each scenario may be separated into its own ATP document, tailored to include actual results founds during testing, and will be subject to the approval of the State 911 Department.

Test Item Number	**Test Title**	**SRD Reference**	**Test Type**
1	ECRF/LVR Functional Test	8.13.3.2	Demonstration
Contract Name	**Contract Number**		
MA NG9-1-1	TBD (template/example data only)		
State 911 Department Support / Windstream Support – May be required Template/example data only – GDIT engineers to identify and detail actual steps for each subsystem			
Requirement(s) (Template/Example data only) Geodetic <findService> query using a location within each jurisdiction produces a <findServiceResponse> when the query is sent to the authoritative DDTi ECRF/LVF for that location. • Recursion does not occur • Error response does not occur • <mapping> contents appear correct, including <displayName> and <uri> elements **Required Test Data** Test 1.1: Geodetic <findService> query Test 1.2.1: Geodetic <findService> query with recursive="false" Test 1.2.2: Civic <findService> query with recursive="false" Test 1.3.1: Geodetic <findService> query with recursive="true"			

Test 1.3.2: Civic <findService> query with recursive="true"
Test 1.4.1: Geodetic <findService> query
Test 1.4.2: Civic <findService> query
Test 1.5.1: <findService> query with geodetic coordinates
Test 1.5.2: <findService> query with civic location
Test 1.6.1: <findService> query having geodetic coordinates outside of known jurisdiction but within the coverage region
Test 1.6.2: civic <findService> query matching the coverage region to which the default mapping is associated, but containing a bogus location
Test 1.7.1: <findService> query having geodetic coordinates within an active override polygon
Test 1.7.2: <findService> query having civic location within an active override polygon
Test 1.8: Civic <findService> query
Test 1.9.1: Geodetic <findService> query consisting of a sub service that was not implemented by the authoritative DDTi ECRF/LVF server
Test 1.9.2: Civic <findService> query consisting of a sub service that was not implemented by the authoritative DDTi ECRF/LVF server
Test 1.10: civic <findService> query with validateLocation=true
Test 1.11: civic <findService> query with validateLocation=true, containing a location present in the Roads layer but not Addresses layer
Test Scenario
Scenario 1.1: Map a service to a location using geodetic coordinates by sending query to its authoritative DDTi ECRF/LVF. Launch DDTi ECRF/LVF Test tool and connect to the authoritative server. Send a geodetic query to the DDTi ECRF/LVF server within its jurisdiction. Verify the response sent by the server.
Scenario 1.2: Redirect response generated by sending a <findservice> query with recursive="false" to a non-authoritative DDTi ECRF/LVF
Scenario 1.3: Response generated by sending a <findservice> query to a non-authoritative DDTi ECRF/LVF which supports recursion
Scenario 1.4: Redirect response generated by sending a <findservice> query to a non-authoritative DDTi ECRF/LVF that does not support recursion
Scenario 1.5: Error response generated by sending a <findservice> query using a location outside of know jurisdiction and coverage region to authoritative DDTi ECRF/LVF server
Scenario 1.6: Response generated for a <findService> query when a server is not able to fulfill a request for a given location but is able to respond with a default URI
Scenario 1.7: Response to a <findService> query using a location within an active override polygon
Scenario 1.8: Mapping a service to a location by sending civic findService query to its authoritative DDTi ECRF/LVF
Scenario 1.9: Error response generated for a sub service that has not been implemented by the authoritative DDTi ECRF/LVF server
Scenario 1.10: Response to a civic query with validateLocation=true, containing a location present in the Addresses layer provisioned to that DDTi ECRF/LVF instance

Scenario 1.11: Response to a civic query with validateLocation=true, containing a location present in the Roads layer but not Addresses layer	
Unusual Requirements/Risks	**Support Equipment Identification** **Software Version:** DDTi ECRF/LVF 1.0 **Platform:**

Procedures (Template/Example data only)

Test 1.1: Response sent by authoritative DDTi ECRF/LVF server for a geodetic <find service> query

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the find service query having geodetic coordinates within the jurisdiction
5. Click on Go button on the test tool

Test 1.2.1: Response sent by non-authoritative DDTi ECRF/LVF server for a geodetic <find service> query with recursive="false".

1. Configure non authoritative DDTi ECRF/LVF server such that it supports recursion
2. Launch the test tool
3. Provide the Appstr URI of the above non-Authoritative DDTi ECRF/LVF server.
4. Select the single query tab in the test tool
5. Paste the find service query with recursive="false" having geodetic coordinates within the jurisdiction
6. Click on Go button on the test tool

Test 1.2.2: Response sent by non-authoritative DDTi ECRF/LVF server for a civic <find service> query with recursive="false".

1. Configure non authoritative DDTi ECRF/LVF server such that it supports recursion
2. Launch the test tool
3. Provide the Appstr URI of the above non-Authoritative DDTi ECRF/LVF server.
4. Select the single query tab in the test tool
5. Paste the find service query with recursive="false" having civic location within the jurisdiction
6. Click on Go button on the test tool

Test 1.3.1: Response sent by non-authoritative DDTi ECRF/LVF server for a geodetic <find service> query with recursive="true".

1. Configure non authoritative DDTi ECRF/LVF server such that it supports recursion
2. Launch the test tool
3. Provide the Appstr URI of the above non-Authoritative DDTi ECRF/LVF server.
4. Select the single query tab in the test tool
5. Paste the find service query with recursive= "true" having geodetic coordinates within the jurisdiction
6. Click on Go button on the test tool

Test 1.3.2: Response sent by non-authoritative DDTi ECRF/LVF server for a civic <find service> query with recursive="true".

1. Configure non authoritative DDTi ECRF/LVF server such that it supports recursion
2. Launch the test tool
3. Provide the Appstr URI of the above non-Authoritative DDTi ECRF/LVF server.
4. Select the single query tab in the test tool
5. Paste the find service query with recursive= "true" having civic location within the jurisdiction
6. Click on Go button on the test tool

Test 1.4.1: Response sent by non-authoritative DDTi ECRF/LVF server that does not support recursion for a geodetic <find service> query

1. Configure non authoritative DDTi ECRF/LVF server such that it does not support recursion
2. Launch the test tool
3. Provide the Appstr URI of the above non-Authoritative DDTi ECRF/LVF server.
4. Select the single query tab in the test tool
5. Paste the find service query having geodetic coordinates within the local jurisdiction
6. Click on Go button on the test tool

Test 1.4.2: Response sent by non-authoritative DDTi ECRF/LVF server that does not support recursion for a civic <find service> query

1. Configure non authoritative DDTi ECRF/LVF server such that it does not support recursion
2. Launch the test tool
3. Provide the Appstr URI of the above non-Authoritative DDTi ECRF/LVF server.
4. Select the single query tab in the test tool
5. Paste the Civic find service query within the local jurisdiction
6. Click on Go button on the test tool

Test 1.5.1 – error response generated for a geodetic query sent to authoritative DDTi ECRF/LVF server using a location outside of know jurisdiction and coverage region

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the find service query having geodetic coordinates outside of known local jurisdiction and coverage region
5. Click on Go button on the test tool

Test 1.5.2 – error response generated for a civic query sent to authoritative DDTi ECRF/LVF server using a location outside of know jurisdiction and coverage region

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the find service query having civic location which is outside of known local jurisdiction and coverage region
5. Click on Go button on the test tool

Test 1.6.1: Response generated for a geodetic findservice query using a location outside of know jurisdiction but within the coverage region to authoritative DDTi ECRF/LVF server

1. Ensure that default mapping is configured in the database
2. Launch the test tool
3. Provide the Appstr URI of the Authoritative server
4. Select the single query tab in the test tool
5. Paste the find service query having geodetic coordinates outside of known local jurisdiction but within the coverage region
6. Click on Go button on the test tool

Test 1.6.2: Response generated for a civic <findService> query matching the coverage region to which the default mapping is associated, but containing a bogus location

1. Ensure that default mapping is configured in the database
2. Launch the test tool
3. Provide the Appstr URI of the Authoritative server
4. Select the single query tab in the test tool
5. Paste the civic find service query matching the coverage region to which the default mapping is associated, but containing an invalid location

6. Click on Go button on the test tool

Test 1.7.1: Response generated for a geodetic findservice query using a location within active override polygon

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the find service query having geodetic coordinates for a location within active override polygon
5. Click on Go button on the test tool

Test 1.7.2: Response generated for a civic findservice query using a location within active override polygon

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the find service query having civic location within active override polygon
5. Click on Go button on the test tool

Test 1.8: Response sent by authoritative DDTi ECRF/LVF server for a civic <find service> query

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the find service query having civic location within the jurisdiction
5. Click on Go button on the test tool

Test 1.9.1: Error response sent by authoritative DDTi ECRF/LVF server for a geodetic <find service> query having a sub service that was not implemented by DDTi ECRF/LVF server

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the geodetic find service query within the jurisdiction having a sub service that is not implemented
5. Click on Go button in the test tool

Test 1.9.2: Error response sent by authoritative DDTi ECRF/LVF server for a civic <find service> query having a sub service that was not implemented by DDTi ECRF/LVF server

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the civic find service query within the jurisdiction having a sub service that is not implemented
5. Click on Go button on the test tool

Test 1.10: Response sent by authoritative DDTi ECRF/LVF server for a civic <find service> query with validateLocation="true"

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server
3. Select the single query tab in the test tool
4. Paste the civic<findService> query with validateLocation=true containing a location present in the Addresses layer
5. Click on Go button on the test tool

Test 1.11: Response sent by authoritative DDTi ECRF/LVF server for a civic <find service> query with validateLocation="true" containing a location present in the Roads layer but not Addresses layer

1. Launch the test tool
2. Provide the Appstr URI of the Authoritative server

3. Select the single query tab in the test tool
4. Paste the civic<findService> query with validateLocation=true containing a location present in the Roads layer but not Addresses layer
5. Click on Go button on the test tool

Expected Results (Template/Example data only)

Test 1.1: Correct <findServiceResponse> should be displayed at the bottom of the test tool

- Recursion should not occur
- No error response should be shown
- <mapping> contents should be correct, including <displayName> and <uri> elements

Test 1.2.1: The <redirect> response should be displayed with 'target' attribute indicating the DDTi ECRF/LVF server unique string that should be contacted next, as well as the 'source' attribute indicating the server that generated the redirect response. Error response should not occur.

Test 1.2.2: The <redirect> response should be displayed with 'target' attribute indicating the DDTi ECRF/LVF server unique string that should be contacted next, as well as the 'source' attribute indicating the server that generated the redirect response.

Test 1.3.1: The path element should have more than one via tag entries indicating recursion

- The <findServiceResponse> contains mapping from the authoritative server
- Error response should not occur
- The <mapping> contents should be correct, including <displayName> and <uri> elements

Test 1.3.2: The path element should have more than one via tag entries indicating recursion

- The <findServiceResponse> contains mapping from the authoritative server
- Error response should not occur
- The <mapping> contents should be correct, including <displayName> and <uri> elements

Test 1.4.1: <redirect> response should be displayed with 'target' attribute indicating the DDTi ECRF/LVF server unique string that should be contacted next, as well as the 'source' attribute indicating the server that generated the redirect response. Error response should not occur.

Test 1.4.2: <redirect> response should be displayed with 'target' attribute indicating the DDTi ECRF/LVF server unique string that should be contacted next, as well as the 'source' attribute indicating the server that generated the redirect response. Error response should not occur.

Test 1.5.1: Error response with a <notFound> element indicating that the server could not find an answer to the query should be displayed.

Test 1.5.2: Error response with a <notFound> element indicating that the server could not find an answer to the query should be displayed.

Test 1.6.1: A findServiceResponse having a warning and <defaultMappingReturned> element should be displayed. It should return the default URI

Test 1.6.2: A findServiceResponse having a warning and <defaultMappingReturned> element should be displayed. It should return the default URI

Test 1.7.1: It should produce a <findServiceResponse> with a <mapping> corresponding to the override polygon.

- The <displayName> and <uri> should display information related to override polygons
- Recursion should not occur. The path element should have only one entry

Test 1.7.2: It should produce a <findServiceResponse> with a <mapping> corresponding to the override polygon.

- The <displayName> and <uri> should display information related to override polygons

- Recursion should not occur. The path element should have only one entry

Test 1.8: Correct <findServiceResponse> should be displayed at the bottom of the test tool.

- Recursion should not occur
- No error response should be shown
- <mapping> contents should be correct, including <displayName> and <uri> elements

Test 1.9.1: Error response having serviceNotImplemented elements should be displayed

Test 1.9.2: Error response having serviceNotImplemented elements should be displayed

Test 1.10: Response should display <locationValidation> element. The <valid> element should enumerate those civic address elements that have been recognized as valid by the DDTi ECRF/LVF server and that have been used to determine the mapping

Test 1.11: Response should display <locationValidation> element. Server should indicate in its response which civic address elements it has recognized as valid, which ones it has ignored, and which ones it has checked and found to be invalid

- The <valid> element should enumerate those civic address elements that have been recognized as valid by the DDTi ECRF/LVF server and that have been used to determine the mapping.
- The <invalid> element should enumerate civic address elements that the server attempted to check, but that did not match the other civic address elements found in the <valid> list.

Actual Results (Enter actual test results)

Test 1.1:
Test 1.2.1:
Test 1.2.2:
Test 1.3.1:
Test 1.3.2:
Test 1.4.1:
Test 1.4.2:
Test 1.5.1:
Test 1.5.2:
Test 1.6.1:
Test 1.6.2:
Test 1.7.1:
Test 1.7.2:
Test 1.8:
Test 1.9.1:
Test 1.9.2:
Test 1.10:
Test 1.11:

Comments/Additional Findings

Test Results (Pass/Fail)	**Verified By:**
☐ Pass ☐ Fail	GDIT Engineer: _____ Name Initials Date Customer Sysadmin: _____ Name Initials Date

8.13.3.3. Throughput Acceptance Test

The contractor shall design, conduct, pass, and document system throughput performance tests for the system and each of its components and subsystems (LVF, ECRF, ESRP, CPE, and all other components and subsystems). These tests shall verify that the installed system and subsystems shall meet the expected throughput capability and provide the expected operational speed and growth potential. The amount of throughput to be tested shall be based on the peak number of transactions experienced by the PSAPs, combined with the contractor's claim for system throughput capability. The contractor shall execute and provide a standard benchmark test based on peak load characteristics with a transaction rate corresponding to the system loading information.

The throughput test shall exercise each component of the system.

Shall any failures be identified during the performance test, the contractor will have a reasonable opportunity to correct the deficiencies, after which a retest may be scheduled. The State 911 Department, at its discretion, may require a retest of the failed functions or may elect to require a complete retest. This process will continue until all functions have passed or the system fails to provide the throughput required by the State 911 Department. Bidders shall provide details in the proposal(s) on how acceptance tests will be conducted. Final agreement on test procedures will be accomplished during contract negotiations.

System throughput testing shall last for a minimum of twenty-four (24) hours and shall involve sufficient transactions, simulating 200% peak traffic load, to validate the capabilities of the systems. All subsystems will be exercised during this test. Delays caused by external systems will not be considered a cause for failure. The system shall not crash due to a transaction overload.

GDIT will comply with the RFR specification. A proposed initial Acceptance Test Plan (ATP) for demonstrating throughput is shown below. This Throughput ATP defines the test plan and records test results. The ATP template will be modified to include specific steps for each subsystem installation and will be subject to the approval of the State 911 Department.

Test Item Number	**Test Title**	**SRD Reference**	**Test Type**
1	Throughput Test (template/example data only)	8.13.3.3	Demonstration

Contract Name	**Contract Number**
MA NG9-1-1	TBD (template/example data only)

State 911 Department Support / Windstream Support – May be required
Template/example data only – GDIT engineers to identify and detail actual steps for each subsystem

Requirement(s) (Template/Example data only)
The following test can be performed from the following location: xxx
The following quantity of systems and software will be used to perform the test:

- (1) ESInet workstation, connected to the ESInet management network, running the xxx application
- (1) Network applications/tools in customer environment (list specific tools when available)

Required Test Data
The following account information needs to be obtained:

- ESInet\ESInet_Admins member AD account and password

Applicable service account and password (list specific service account when available)

Test Scenario
Connect to the Network Node using customer approved tools (list when identified).
Open the AFNet BMS application on the IMS workstation. Verify that all screens and reports are functional and displaying valid data.

Unusual Requirements/Risks	**Support Equipment Identification** **Software Version**: DDTi DataRite NXG™ 3.3 **Platform:**

Procedures (template/example data only)

Test 1.1: Packet Loss:

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.2: Latency:

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.3: Jitter:

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.4: Routing (depending on system being tested, may be network packet routing or call routing):

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only)
   LIST each command
   used to execute code
   needed to complete test
6. Exit

Test 1.5: Simulate 200% of Peak Traffic:

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2
3. Perform step 3
4. Perform step 4

5. Execute the following code (example only) LIST each command used to execute code needed to complete test 6. Exit
Expected Results (template/example data only) **Test 1.1:** Monthly average packet loss between demarcation points not to exceed 0.5% **Test 1.2:** Packet Latency to an average round trip time of forty (40) milliseconds which equates to a one (1) way transmission time of twenty (20) milliseconds (Packet Latency is measured between the demarcation points, typically between a data center demarcation point and a PSAP demarcation point) **Test 1.3:** Jitter - shall not exceed twenty (20) milliseconds **Test 1.4:** Verify network packets and/or test calls route as required **Test 1.5:** System performs optimally under 200% of peak traffic load for a minimum of 24-hours
Actual Results **Test 1.1:** **Test 1.2:** **Test 1.3:** **Test 1.4:** **Test 1.5:**
Comments/Additional Findings

Test Results (Pass/Fail)	**Verified By:**
☐ Pass ☐ Fail	GDIT Engineer: _____ Name Initials Date Customer Sysadmin: _____ Name Initials Date

8.13.3.4. Availability Acceptance Test

Bidders shall describe how they will test the installed system, including all subsystems, to ensure that the system performs at a 99.999% level of availability and to ensure that the system allows for all 911 payloads to be delivered to a PSAP. The availability test shall last a minimum of sixty (60) days and shall be conducted for each of the following:

A. Hardware and related equipment;

B. Software; and

C. and ESInet availability.

Hardware and related equipment provided by the contractor shall perform at a 99.999% level of availability, with a maximum of two (2) periods of down time resulting from hardware or related equipment failures.

The contractor shall test software during the same time period. A maximum of two (2) software component failures will be permitted during the testing period. Shall the same software component fail more than once during the test, the contractor shall correct or replace the software component. The repair/maintenance procedures in effect during the test shall be the same repair/maintenance procedures that shall be in effect during normal system operation after site acceptance.

Any corrective redesign necessary to meet reliability and availability requirements shall be the sole responsibility of the contractor, and shall be accomplished without cost to the State 911 Department.

Bidders shall describe in detail how acceptance testing shall be conducted. The final system testing procedures shall be subject to the approval of the State 911 Department

GDIT will comply with the RFR specification. A proposed initial Acceptance Test Plan (ATP) for demonstrating availability is below. This Availability ATP defines the test plan and records test results. The ATP template will be modified to include specific steps for each subsystem installation and will be subject to the approval of the State 911 Department.

Test Item Number	**Test Title**	**SRD Reference**	**Test Type**
1	Availability ATP (template/example data only)	8.13.3.4	Demonstration

Contract Name	**Contract Number**
MA NG9-1-1	TBD (template/example data only)

State 911 Department Support / Windstream Support – May be required
Template/example data only – GDIT engineers to identify and detail actual steps for each subsystem

Requirement(s) (template/example data only)
The following test can be performed from the following location: xxx
The following quantity of systems and software will be used to perform the test:

- (1) ESInet workstation, connected to the ESInet management network, running the xxx application
- (1) Network applications/tools in customer environment (list specific tools when available)

Required Test Data
The following account information needs to be obtained:

- ESInet\ESInet_Admins member AD account and password

Applicable service account and password (list specific service account when available)

Test Scenario
Connect to the Network Node using customer approved tools (list when identified).
Open the AFNet BMS application on the IMS workstation. Verify that all screens and reports are functional and displaying valid data.

Unusual Requirements/Risks	**Support Equipment Identification** **Software Version:** DDTi DataRite NXG™ 3.3 **Platform:**

Procedures (template/example data only)

Test 1.1: Availability of Hardware:

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2 (GDIT engineer to define procedures to capture 60-day test)
3. Perform step 3
4. Perform step 4
5. Execute the following code (example only—engineer to replace with actual steps)
   SELECT name
   FROM master…sysdatabases
   WHERE convert(sysname,DatabasePropertyEx([name],'Status')) = 'ONLINE'
   ORDER BY name
6. Exit

Test 1.2: Availability of Software:

1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps)
2. Perform step 2 (GDIT engineer to define procedures to capture 60-day test)

3. Perform step 3 4. Perform step 4 5. Execute the following code (example only—engineer to replace with actual steps) SELECT name FROM master…sysdatabases WHERE convert(sysname,DatabasePropertyEx([name],'Status')) = 'ONLINE' ORDER BY name 6. Exit **Test 1.3: Availability of ESInet:** 1. Log into xxx using the xxx-adm account. (Need technical input for remaining steps) 2. Perform step 2 (GDIT engineer to define procedures to capture 60-day test) 3. Perform step 3 4. Perform step 4 5. Execute the following code (example only – engineer to replace with actual steps) SELECT name FROM master…sysdatabases WHERE convert(sysname,DatabasePropertyEx([name],'Status')) = 'ONLINE' ORDER BY name 6. Exit
Expected Results (template/example data only) **Test 1.1:** Hardware availability shall be 99.999% over a period of 60 days **Test 1.2:** Software availability shall be 99.999% over a period of 60 days **Test 1.3:** ESInet network availability shall be 99.999% over a period of 60 days
Actual Results **Test 1.1:** **Test 1.2:** **Test 1.3:**
Comments/Additional Findings

Test Results (Pass/Fail)	**Verified By:**
☐ Pass ☐ Fail	GDIT Engineer: _____ Name Initials Date Customer Sysadmin: _____ Name Initials Date

8.13.4. Installation Support

The contractor shall provide specialized technical service personnel to provide support in all areas of the project, to include but not be limited to, communications, computer hardware and software, equipment service and repair, as required by the project work plan. All technical service personnel shall be fully qualified in their respective disciplines. All costs associated with the provision of the technical support services, if any, are to be included in the proposal.

GDIT will comply with the RFR specification.

The GDIT team includes all system engineering and technician resources to cover all service disciplines necessary to design, deploy, and support the NG9-1-1 configuration for the Commonwealth of Massachusetts. In addition to Subject Matter Experts (SME) from each of the OEMs who will be part of this project design and implementations, GDIT has numerous certified SME engineers with extensive implementation experience in specialized areas such as E9-1-1 systems, Cisco networking, security prevention and detection systems, Oracle Session Border Controllers (BCF), TDM and PBX systems, and data center engineering. Table 28 provides details for the technical disciplines possessed by the GDIT team.

Table 28. GDIT Team Technical Disciplines

Technical Discipline	Technology	Responsibilities
Systems Engineer	All	Technical resource responsible for complete Integration of the Commonwealth of Massachusetts NG9-1-1 solution
Facility Engineer	Facility Subsystems	Technical resource responsible for review of PSAP, NSOC, and data center facility HVAC, grounding, and AC electrical subsystems for adequacy in supporting each location's NG9-1-1 equipment suite
Telecommunication Engineer	Circuit Switch and Telecom Systems	Technical resource responsible for review and integration of legacy TDM interfaces into the NG9-1-1 architecture to include selective router trunk circuits and legacy administrative telephone systems at each PSAP site
Systems Engineer	Border Control Function (BCF)	Technical resource responsible for design, configuration, and integration of the BCF into the NG9-1-1 solution
Systems Engineer	Emergency Services Routing Proxy (ESRP)	Technical resource responsible for design, configuration, and integration of the ESRP into the NG9-1-1 solution
Systems Engineer	Legacy Network Gateway (LNG) / Legacy PSAP Gateway (LPG)	Technical resource responsible for design, configuration, and Integration of the LNG and LPG functional elements into the NG9-1-1 solution
Systems Engineer	Protocol Interworking Function (PIF)	Technical resource responsible for design, configuration, and integration of the PIF into the NG9-1-1 solution
Systems Engineer	Emergency Call Routing Function (ECRF)	Technical resource responsible for design, configuration, and integration of the ECRF into the NG9-1-1 solution
Systems Engineer	Emergency Call Routing Function (ECRF) / Location Verification Function (LVF)	Technical resource responsible for design, configuration, and integration of the ECRF/LVF into the NG9-1-1 solution
Systems Engineer	IP PBX/PSAP CPE	Technical resource responsible for design, configuration, and integration of the IP PBX/PSAP CPE into the NG9-1-1 solution
Systems Engineer	Digital Logging Recorder (DLR)	Technical resource responsible for design, configuration, and integration of the DLR into the NG9-1-1 solution
Systems Engineer	Network Appliances/Services	Technical resources responsible for design, configuration, and integration of network appliances and services for the NG9-1-1 solution to include: Layer 2 switching, routers, storage, NTP, DNS, DHCP, etc.
Systems Engineer	Data Center/PSAP Connectivity	Technical resources responsible for design, configuration, and integration for the network and associated circuits providing connectivity between the data center locations and PSAP sites
Systems Engineer	Management Applications	Technical resource responsible for design, configuration, and integration of management applications into the NG9-1-1 architecture
Installation Technicians	All	Technical resources responsible for the physical installation and initial power-up of all NG9-1-1 components at their designated locations within the Commonwealth of Massachusetts

Technical Discipline	Technology	Responsibilities
Field Service Technicians	All	Resources responsible for the repair and maintenance of deployed NG9-1-1 system

8.13.5. Description of Procedures

The contractor shall provide and maintain a description of procedures for quality control. To the extent necessary, written inspection and test procedures shall be prepared to supplement the applicable drawings and specifications, and shall make clear the manner in which such inspection and test procedures are to be used.

Software development shall include model statements, data-flow diagrams, data dictionary, process specification, and object-relationship diagrams. The contractor shall employ all accepted software development criteria and procedures. The description of the quality control system and all applicable inspection and test procedures shall be available to the State 911 Department prior to system acceptance.

GDIT will comply with the RFR specification.

Our ISO 9001:2008 certification requires GDIT to have documented, repeatable processes to ensure our ability to continue producing quality services and products, including software development. GDIT's Quality Management System (QMS) is keenly focused on infusing our Quality and Environmental Health and Safety (QEHS) into every aspect of our day-to-day work activities. The GDIT team has extensive experience providing information technology, networking, security, and telephony solutions and services to our customers, affording us an opportunity to transition a mature and proven QMS program to accommodate our customer's needs. We have implemented numerous procedures to enhance our processes, highlighted in Table 29 below. GDIT will provide a draft QCP, including a description of our quality control system and applicable inspection and test procedures, to the Commonwealth for review and approval post-award.

For Software Development Quality Procedures that will be employed, refer to Section 8.11.3, Software Integrity Controls.

Table 29. The Foundations of GDIT's Quality Management System

Area of Focus	Quality Assurance Action
Personnel	Select people with proper skills and certifications
	Customer training tailored specifically for the customer's operational and mission needs
Procedures	ISO 9001:2008 certified procedures embedded as a way of doing business
	Customer-approved plans
Design	Perform reviews (e.g., preliminary design review and final design review, peer-to-peer, supervisory, and customer reviews)
	OEM product evaluations
Testing	Conduct system testing following design approval as agreed to by the State and GDIT
Site Surveys	Conduct site surveys. Prepare site-specific architecture to accommodate Local Exchange Carrier (LEC), county, and legacy equipment slated for re-use
System Pre-Deployment	Configured system load testing and burn-in
	Simulation modeling
Installation	In-progress and final inspection
	Nonconforming product detection and segregation
Final Inspection	Customer observance of or participation in final inspection and testing
	Integrated system testing
Information Assurance	Conduct site-specific IA activities in accordance with Performance Work Statement

Area of Focus	Quality Assurance Action
	(PWS) and contractual requirements
Post-Installation	Documented drawings and test results to customer
	Lessons learned to team members, customers, and OEMs
	System performance tracking and trend analysis during warranty period

8.13.6. Storage

The contractor shall provide adequate procedures for storage and control of supplies to be used under the contract to ensure preservation and treatment in accordance with applicable requirements. Procedures shall define inspections to be conducted at scheduled intervals. Storage facilities shall be the responsibility of the contractor. Storage at any Commonwealth or other public facility shall not exceed three (3) days unless previous approval by the State 911 Department has been received.

GDIT will comply with the RFR specification.

GDIT will store project material at its i3 Solutions Interoperability Lab facility located in Needham, Massachusetts and other facilities located strategically throughout the Commonwealth to meet availability and operational requirements. All project material delivered to our facilities will be inventoried and visually inspected. In addition to the visual inspection, all active components will go through a Pre In-service Test and Checkout (PITCO) as part of lab staging that involves:

- Initial power-up of the active component to validate power supply integrity
- Cooling fan check, if applicable
- Successful initial login, if applicable
- Hard drive check, if applicable
- Testing of all ports on the chassis, such as CD/DVD drive, USB, 10/100/1000, system peripherals (video, keyboard, mouse), and console

The intent of the visual inspection and PITCO process is to proactively identify and resolve any out-of-box failures/non-compliant material early in each staging phase. Items that do not pass inspection and PITCO will be segregated from conforming material items to avoid use when system staging commences. Non-conforming material will be replaced.

Throughout the staging and PSAP pre-deployment time frame, GDIT will conduct regularly scheduled inventories and inspections as defined in our Project Plan. After successful completion of staging and once authorization is granted by the State 911 Department, GDIT will package and ship components to their final installation site. GDIT plans to store equipment at its designated installation site for no more than three days prior to the start of its physical installation. If this is not feasible due to space constraints or security concerns, GDIT has dedicated secure storage space within its Needham facility where equipment can be stored, or we will make arrangements with a local storage facility to provide suitable secure storage until such time as the approved schedule dictates when the material needs to be moved to a location for installation.

8.13.7. Quality Control Records

The contractor shall maintain adequate records of inspections and tests throughout all stages of contract performance, including checks made to ensure accuracy of inspection and testing equipment and other control media. All quality control records shall be available for review by the State 911 Department, and copies of

individual records shall be furnished to the State 911 Department upon request. The contractor shall furnish records requested within ten (10) business days of the request.

GDIT will comply with the RFR specification.

In conjunction with our existing ISO 9001 Quality Management System (QMS) practices, GDIT will develop MA NG9-1-1 project specific quality control records and processes that will address checks, inspections, tests, and also our own external audits to be performed by personnel not involved with this project.

GDIT will maintain the following quality control records:

- Material receiving reports
- Pre In-service Test and Checkout (PITCO) checklists
- Serial number spreadsheet
- Acceptance test results
- Test equipment calibration records

Upon request, records will be provided to the State 911 Department. Records will be furnished within 10 business days of the request.

8.13.8. Corrective Action

The contractor shall take prompt action to correct conditions that might result in defective supplies or services. The contractor shall make use of feedback data generated and furnished by user activities, as well as that generated in the contractor's facility.

GDIT will comply with the RFR specification.

Non-conforming material identified prior to on-site activities will be replaced by GDIT. GDIT will coordinate with the appropriate vendor/OEM to have the non-conforming material replaced when identified. Once systems are installed in the field, GDIT will utilize feedback generated by tests/inspections and users to address issues requiring corrective action. Items failing tests/inspections will either be replaced (if defective) or reconfigured. User feedback will be used to optimize the system configuration.

8.13.9. Resistance to Interference

The system shall not suffer from interference or measurable performance degradation from use of installed console devices, public safety radio transceiver equipment, microwave communication systems, other installed data processing equipment, or any other devices present in the system's operational environment

GDIT will comply with the RFR specification.

NG9-1-1 component performance will not be negatively affected by existing systems installed in the operational environment.

8.13.10. Emissions Criteria

The system shall not cause interference to the existing radio, security, or closed circuit television communications systems, installed communications console equipment, or other data processing equipment present in the operational environment, and, in addition, shall comply with all applicable FCC standards as applied to data processing equipment.

GDIT will comply with the RFR specification.

GDIT's proposed solution will not interface with legacy systems installed in the operational environment and complies with all applicable FCC standards as applied to data processing equipment.

8.13.11. Responsibility for Contractor Equipment

Contractors shall assume complete responsibility for all tools, test equipment, or other items that are the property of the contractor and are being used during equipment installation. The State 911 Department will not be responsible for lost or damaged items that the contractor may leave at work sites for their own convenience.

GDIT will comply with the RFR specification.

GDIT assumes responsibility for all tools, test equipment, and other items used during the project that are the property of GDIT and its team. GDIT agrees that the State 911 Department is not responsible for lost or damaged items that may be left at work sites by GDIT or its team for their own convenience.

8.13.12. Testing of Equipment and Construction

The State 911 Department reserves the right to inspect and test all materials and equipment used in the construction of the project in accordance with accepted standards. The laboratory or inspection agency shall be selected by the State 911 Department. The State 911 Department will pay for all laboratory inspection services.

Materials of construction, particularly those upon which the strength and durability of structures may depend, shall be subject to inspection for suitability for the use intended.

The contractor shall maintain quality assurance and control in a manner consistent with industry practices and as specified.

The State 911 Department may, at reasonable times, inspect the installed equipment at the data centers, training centers, and PSAPs.

GDIT will comply with the with the RFR specification.

GDIT will support all tests and inspections conducted by the State 911 Department throughout the project life cycle.

8.13.13. Protection of Work and Property

The contractor shall continuously maintain adequate protection of all work from damage, and shall protect the State 911 Department's and/or any other property from injury or loss arising in connection with the contract. The contractor shall adequately protect adjacent property as provided by law and the contract.

The contractor shall provide and maintain all passageways, guard fences, lights, and other facilities for protection required by public authority and local conditions. This requirement applies only to site(s) that are controlled by the contractor.

GDIT will comply with the with the RFR specification.

For locations controlled by GDIT, the GDIT team will employ safety and security measures to protect installation materials and workmanship from damage. The installation/testing effort will not compromise any site's existing physical security.

8.13.14. Validation Testing Documentation

Bidders shall, for each functional element of the system, include in the response a complete set of validation testing documentation. Such documentation shall be sufficient to identify all elements performing a function as required to fulfill the role of each functional element in sufficient detail to allow analysis of the adequacy of the proposed element by the State 911 Department.

The contractor shall provide an updated (then current) suite of validation test documentation for actual installation. The State 911 Department reserves the right to determine the adequacy of the validation testing documentation and procedures.

GDIT will comply with the RFR specification.

GDIT has established an integration laboratory designed to validate the integration and functional aspects of our partner products. The laboratory environment provides GDIT, our partners, and prospective customers the assurance of technical interoperability across a wide range of functional elements and applications. It also provides the opportunity for development of expertise in implementation and sustainment in a multi-product environment.

GDIT will perform testing and inspections of all systems solutions to ensure the technical functionality and accuracy of all work, including reports and other documents required in support of that work. Testing will be performed in accordance with OEM installation manuals, practices, and the appropriate vendor's test procedures. The testing will ensure the system is fully functional and meets the user requirements.

GDIT will provide a comprehensive and unified test plan as part of the implementations documentation in accordance with the RFR specifications. GDIT will identify and provide approved industry and OEM procedures that outline, sequence, and indicate qualifications for system acceptance (i.e., 24-hour burn-in, etc.). These procedures will ensure the system is fully functional and meets the user requirements. GDIT will conduct testing of the complete system, including premise equipment, distribution systems, network equipment, software, appliance functionality and operating support systems, as agreed to.

Our draft validation testing cases and documentation, which addresses functional element test and validations, are described in detail in Sections 8.13.1 through 8.13.3. Our final Acceptance and Test Plans (ATPs) will be further defined and developed in-line with the actual installation plan that will be coordinated with the State 911 Department and validated.

8.13.15. Site Cutover Project Plan and Advanced Notification Documentation

For each PSAP and training center, the contractor shall provide the State 911 Department with a generic Site Cutover Project Plan beginning with the initial site survey visit and culminating with the site acceptance. The contractor shall provide a generic Site Survey Form that is identical to or equivalent to the Site Survey Form attached hereto as Attachment M- Site Survey Form. The contractor shall include in the plan a chronology of the work activities that will occur at the PSAP/training center as well as the identity and role of the subcontractors who will be on-site and the tasks they will be performing. The contractor shall include in the plan an outline of the events that will occur on a daily basis, a detailed procedure for taking the PSAP offline for said work, if necessary, and a list of the responsibilities of PSAP staff in connection with the cutover. The contractor shall also provide in this plan a backup procedure to ensure that all vulnerable data has been appropriately backed up after all configurations are final, which shall be completed at least forty-eight (48) hours prior to the scheduled cutover date.

The State 911 Department will coordinate with the PSAP and the contractor the initial site visit at least sixty (60) days prior to cutover. The following project team representative shall attend the initial site visit:

- *The contractor's Project Manager and field technician, who shall identify any changes to the Site Install Project Plan and potential problems related to the installation;*
- *A State 911 Department representative, who shall be responsible for authorizing any changes in configuration that are made to the Site Cutover Project Plan as a result of the initial site visit; and*
- *The PSAP administrator or designee, who shall review the Site Cutover Project Plan during the initial site visit and identify any changes in site configuration since the initial site survey.*

During the initial site visit the following items, at a minimum, will be discussed:

- *Site Cutover Project Plan;*
- *Electrical requirements;*
- *Location/placement of equipment;*
- *Autodial list;*
- *PSAP responsibilities;*
- *Electrical Permit form; and*

Location of circuits and equipment.

The contractor shall note any necessary changes identified during the initial site visit, and such changes require approval by State 911 Department. The contractor shall provide the State 911 Department with a copy of the notes from the initial site visit before any installation can commence on the identified changes.

The State 911 Department representative shall conduct periodic site visits to check on the status of the cutover. The PSAP administrator or designee shall be available during the cutover to address any site-specific questions from the contractors.

GDIT will comply with the RFR specification.

For each PSAP and training center, GDIT will provide three individual deliverables as part of the site documentation package:

- Generic Site Cutover Project Plan
- Site Survey Checklist
- Site-Specific Cutover Plan

The generic Site Cutover Project Plan, furnished in both MS Project (latest version) and Adobe PDF format, encompasses all tasks between initial site survey and site acceptance necessary to successfully deploy NG9-1-1 equipment suites associated with a PSAP or training center location. It functions as the prime management tool for each PSAP/training center deployment. GDIT's Site-Specific Cutover Plan will also include detailed and chronological step-by-step procedures for any system or service cutover. Our Methods of Procedures (MOP) will also be validated with the State 911 Department well before the scheduled cutover date. All tasks are assigned to a distinct project phase to include:

- Engineering/Planning Phase
- Staging Phase
- Site Implementation Phase
- Cutover Phase

Successful completion of each phase is a prerequisite to the next phase commencing. Measurable milestones are used within each phase to define successful completion and resources are assigned to all tasks. Development of the final approved Site Cutover Project Plan is a collaborative effort between the GDIT team, the State 911 Department, and local PSAP site representatives. It reflects task sequencing, dependencies, and time frames synchronized with stakeholder resource allocations, site availabilities, and other parameters unique to the site deployment. Once approved, the Site Cutover Project Plan will be used by the GDIT project manager to measure project status through overall project completion.

GDIT will develop a site survey checklist, equivalent to the Site Survey form attached as Attachment M. GDIT's version of the checklist expands on the details contained in the Attachment M form and will be used by each survey team to document the current site

conditions and collect the data necessary to fine tune the system design, complete required design documentation, and document facility readiness.

The initial site visit, through coordination with the State 911 Department, will occur at least sixty (60) days prior to the actual cutover milestone event. GDIT's survey team, at a minimum, will include our Project Manager and field technician. GDIT may also request that additional engineering/technician resources be included as part of the survey team for the larger PSAP sites, such as Boston and Framingham. Pictures will be taken, where allowed, to further support data collected on the checklist. Our survey team(s) will systematically collect and verify data for the current site conditions, detailing such information as:

- Facility AC power, grounding, generator, and Heating, Ventilation, and Air Conditioning (HVAC) subsystems
- Equipment room layouts and available footprint
- Legacy dispatch systems
- Legacy administrative communication system
- CLEC termination data for selective router trunks
- Cable paths and supporting infrastructure for new cabling

The following categories will be included in survey checklists for each location:

- Basic site information to include address, site Point of Contact (POC) information, and any special access requirements specific to the location
- PSAP responsibilities
- Facility details:
  - HVAC: Data will be gathered on the make, model, age, physical appearance, and BTU/hour for the HVAC systems that provide environmental support for the facility/equipment room. The team will also note whether the HVAC configuration is redundant. The data collected will be compared against the total designed heat loads for the planned equipment suite to verify that the existing HVAC systems are adequate.
  - Electrical: The team will document which aspects of the existing electrical infrastructure can be re-used for the new equipment. If new circuits are required, the survey team will document the following:
    - Make, model, rating, and other technical details for the power panel identified by the team for use.
    - Available circuit breaker positions within the panel. The team will completely document the panel schedule.
    - Circuit breaker types that can be used within the panel.
    - Determine whether the panel is tied to emergency power (i.e., generator).
    - Document conduit paths from the panel to the new equipment suite.

- Permitting requirements.

— Grounding: The existing ground connection point will be assessed for suitability in supporting the grounding requirements of the new equipment.
— Generator: Data will be gathered on the make, model, and size of the generator system in place at each location.
— Gather data for any UPS make and model, age, and battery strength if possible.
— Building Codes: Document any building codes that must be met for the site design.

- Equipment Room Details:

— Floor and Wall Types: The types of floors and walls in each equipment room will be noted. This information is documented in case there are special considerations that must be accounted for with respect to physical installation (i.e., raised floor, etc.).
— Floor Plan Layout: The current layout of each equipment room will be documented to include room dimensions and dimension data related to all equipment installed within the room. Open floor space will be noted for the installation of new equipment. At each PSAP, a location will also be noted for the termination demarcations for ESInet Wide Area Network (WAN) links from the data centers.

- Legacy System Details:

— Call Taker Positions: Legacy PSAP call taker position configurations will be documented to include:

- Make, model, and quantity
- Cabling details
- Autodial lists
- The information collected is used to provide specific de-installation details on project documentation, such as project drawings and the required de-installation plan

— Dispatch Systems: Legacy dispatch system configurations for Land Mobile Radio (LMR) and Computer-Aided Dispatch (CAD) will be noted to include:

- Make, model, and quantity
- Cabling details
- Information collected on legacy dispatch systems is used by the engineering team to finalize integration methodology between these systems and new local recording components

— Administrative Communication System: the legacy telephone switch architecture at each PSAP site will be noted to include:

- OEM, software version, and total number of lines in service. Number of lines in service will be broken down by subscriber type if this information is available.

- Termination point for telephone lines.

- If a local switching system is not present, the team will note who the dial tone provider is for the facility.
- Information collected on legacy telephone systems is used by the engineering team to finalize integration methodology between these systems and new local recording components.

— Selective Router Trunk Terminations:

- Termination data related to local selective router trunk terminations at each PSAP will be noted to include: circuit IDs and servicing CLEC information

- Cable Path Details:

— Paths for new cabling will be documented by the survey team. Existing paths will be used to the maximum extent feasible. Information collected by the team includes:

- Plenum versus non-plenum space
- Cable ladder configurations, if used, and whether additional ladder is needed
- Distances between equipment and termination points to properly design final cable lengths

In addition to data collection, GDIT will discuss the following during the initial site visit:

- Site Cutover Project Plan
- Electrical/facility requirements
- Equipment location
- PSAP configuration details
- PSAP roles/responsibilities
- Circuit demarcation points

Once all data is compiled, GDIT will turn over a copy of the site survey checklist to include pictures to the State 911 Department. The checklist will document any changes identified during the survey to facilitate review and approval of these changes by the State 911 Department.

GDIT will also develop a detailed cutover plan as part of the documentation package for each site. The cutover plan will contain the following sections:

- **System Description:** This section provides a technical description of the system to be cutover.
- **Cutover Prerequisites:** This section details all prerequisites that must be met/completed before cutover can be authorized.
- **Cutover Procedure:** This section described the procedure to be employed to transition service to the NG9-1-1 architecture.
- **Risk Definition and Mitigation Plan:** This section identifies cutover risks and the strategies that will be used to mitigate them.
- **Contractor Responsibilities:** This section outlines all GDIT responsibilities related to prerequisites and cutover.

- **PSAP/State 911 Department Responsibilities:** This section outlines all PSAP and State 911 Department responsibilities related to prerequisites and cutover.
- **CLEC Responsibilities**: This section outlines all CLEC responsibilities related to prerequisites and cutover.
- **Project Phasing:** The project phasing section documents contact information for key cutover personnel and contains checklists for:
  - Pre-cutover prerequisites with required dates for completion and resource assignments
  - Cutover, with start times and resource assignments. Tasks that require downtime are depicted using red text to separate them from activity that does not affect service.
- **Recovery and Fallback:** This section outlines recovery and fallback procedures should it be necessary to transition back to the legacy system architecture.

8.13.16. ESInet Circuit to PSAP Testing

The contractor shall design, conduct, pass, and document a thorough test procedure for the network and network monitoring components of the system. This test plan shall at minimum, confirm that these components meet the specifications in the RFR as well as any other requirements necessary for the compliance with applicable standards, rules, and regulations.

This shall include, but not be limited to, tests for:

- *End-to-end connectivity of all circuits;*
- *Throughput;*
- *Packet loss;*
- *Latency;*
- *Jitter;*
- *Routing;*
- *QoS mechanisms;*
- *Fault recovery;*
- *Fail-over from primary to secondary paths;*
- *Simulation of peak traffic load for a minimum of twenty-four (24) hours;*
- *Network monitoring systems;*
- *Faulty notification systems; and*
- *Firewalls and intrusion detection systems.*

The contractor shall, fifteen (15) days prior to the cutover date, test each circuit connection to the PSAP. The testing shall be thorough and the testing shall include the generation of simulated traffic to detect anomalies regarding proper connectivity to the ESInet, packet loss, latency, jitter, QoS, routing, traffic engineering, and other specifications set forth in the RFR or otherwise required for the operation of the system. For those PSAPs that have more than one ESInet connection, either through diverse entries or carriers, the circuit fail over shall also be tested at this time. The contractor shall, within three (3) days of completion of testing, submit to the State 911 Department documentation in a form satisfactory to the State 911 Department that all circuits have been successfully tested. The documentation shall include, for all circuits, the following information: carrier, circuit ID, type, speed, testing date, and location.

If any of the ESInet tests fail, the contractor shall, within (5) days, correct the deficiency, retest the circuits, and submit to the State 911 Department documentation in a form satisfactory to the State 911 Department that all circuits have been successfully tested. The documentation shall include, for all circuits, the following information:

carrier, circuit ID, type, speed, testing date, and location. If the test fails a third time, the contractor shall submit, within forty-eight (48) hours, a remediation plan to the State 911 Department for approval.

GDIT will comply with the RFR specification.

GDIT will develop and perform a comprehensive set of tests for the network and network monitoring components of the NG9-1-1 system architecture. The goal of testing will be to confirm functional network performance and compliance with applicable specifications listed in the RFR. The test program initiated for the network and network monitoring will include:

- Basic end-to-end connectivity from the data center demarcation to the PSAP demarcation for each circuit
- QoS verification with respect to throughput, packet loss, latency, and jitter
- Circuit redundancy with respect to fault recovery and path redundancy
- Traffic simulation of peak traffic for a 24-hour period to validate circuit performance
- Network monitoring system functionality
- Fault notification functionality
- Network security functionality (i.e., firewall and intrusion detection)

Fifteen (15) days prior to the scheduled site cutover date, GDIT will fully test each ESInet connection to the PSAP. The circuit testing program will be in accordance with the approved circuit test plan, inclusive of the minimum test elements described in the previous bullets above. No later than three (3) days after completion of testing, GDIT will submit circuit test results to the State 911 Department for all circuits tested. The test report will be developed in a format satisfactory to the State 911 Department and will include, at a minimum, carrier information, circuit ID, circuit type, speed, test date, and test location.

GDIT will address and correct any deficiencies that result in a failed test for the ESInet circuit(s). These corrective action(s), to include circuit retest and test documentation submittal, will be corrected within five (5) days of the failed test. Should a third failure be experienced, GDIT will submit a remediation plan to the State 911 Department within forty-eight (48) hours of the failed test.

8.13.17. Staging Requirements

The contractor shall provide a staging process for the installation of new CPE and shall perform the following steps as part of that process:

A. Install and configure all components for each PSAP or training center in a staging area, within the Commonwealth of Massachusetts, designated by the contractor; and

B. Power on equipment, verify configuration settings and burn system in for a minimum of seventy-two (72) hours.

The State 911 Department shall have access to staging area for inspection at any time.

GDIT will comply with the RFR specification.

GDIT will perform staging of new CPE at its i3 Solutions Interoperability Lab in Needham, Massachusetts.

GDIT's staging effort involves completion of multiple steps ranging from initial material inspections to burn-in. GDIT's factory staging Concept of Operations (CONOPS) includes:

- **Initial inspection and Pre-In-Service Test and Checkout (PITCO):** All material delivered to GDIT's i3 Solutions Interoperability Lab Needham will be visually inspected for damage and compliance with the material order. Active components will undergo PITCO to validate basic functionality. Items that pass inspection and PITCO will be used in the staging effort. Items that fail will be deemed non-conforming and replaced.
- **Physical Installation and Power-up:** After inspection and PITCO, all components will be physically installed within the lab environment. This includes rack and stack and initial power-up of active components. System cabling is also installed, terminated, and labeled during this part of the staging process.
- **System Configuration:** During this step in the staging process, configuration details are programmed for the CPE to include at a minimum:
  - Workstation setup to include:
    - Operating system installation/patching
    - Windows login setup
    - Anti-virus installation/configuration
  - Network integration for the workstation for IP address/VLAN/subnet schemes NTP, Syslog, Active Directory, etc.
  - Integration between Workstation, Polycom IP telephone, and AIU unit
  - 9-1-1 call taker logins
  - Autodial setups
  - Back-office equipment configuration for the site's UPS, IP router/Ethernet switch, and managed PDU:

Since the majority of PSAP sites and training centers will be staged after the data centers are deployed, GDIT will engineer, furnish, and install WAN circuits between the two designated data center sites and GDIT's i3 Solutions Interoperability Lab. These circuits allow the staged equipment suite at the lab to integrate with the hosted applications at the data centers. These circuits will remain in place until staging for the last PSAP and/or training center is completed.

- Acceptance Test Dry Run:
  - Once system configuration is completed, GDIT will conduct a dry run for required acceptance tests.
- Acceptance Test/Burn-In:
  - During this stage in the process, GDIT will perform acceptance testing for the CPE. A 72-hour burn-in will also be performed on the equipment.
- Staging Breakdown/Packing:

— Upon completion of acceptance testing and burn-in, GDIT will break down the staged equipment suite and prepare it for shipment to its final installation location

Our i3 Solutions Interoperability Lab in Needham will be accessible to the State 911 Department for inspection at any time.

8.13.18. Full System Staging Test

The contractor shall, at least forty-eight (48) hours prior to the installation at the PSAP or training center, provide the State 911 Department with the results of the full system staging test that describes any component failures encountered and on what test attempt the system passed the test. Staging shall include configuration work for Auto-Dial entries and user logins. The full system staging test documentation shall include all the test steps identified in the pre-cutover test portion of the functionality checklist with the addition of pass/fail metrics, measurement criteria used to determine pass/fail metrics, and the results of all system test procedures conducted by the contractor during staging. Such documentation shall include the number of times the system was tested, on what attempt the system passed, and the repairs performed to address test result failures.

The contractor shall:

If a component fails, replace the component;

If the replacement fails or similar component fails, refer the issue to the Technical Support team of the manufacturer of the component for review and repair;

If a component failure is encountered during testing and the component is considered a system-wide resource, restart full system test once the repair is made; and

If the component is a single isolated component such as a workstation, restart testing relevant to the workstation.

GDIT will comply with the RFR specification.

Forty-eight (48) hours prior to site deployment at the PSAP or training center, GDIT will provide the State 911 Department with the results of testing conducted during the staging the process. The submitted test result report will include the following:

- Test steps as identified in the pre-cutover test section of the functionality checklist. Testing conducted during staging includes:
  - Hardware/software redundancy
  - System functionality and routing
  - System login and auto-dials
  - Integration tests as applicable between NG9-1-1 functional elements
- Pass/fail metrics including criteria for defining pass/fail for the particular test
- Test results

The test results portion of the test report will document:

- The number of times the test was conducted. The attempt in which the test passed will be noted.
- Description of and reasons for failures on a particular test. Corrective actions taken to address the failure will be noted.

Defective components will be isolated and replaced. As necessary, GDIT will elevate issues to the technical support team of the component Original Equipment Manufacturer (OEM) for

resolution. Components considered system-wide will result in a restart of the full system test once repaired/replaced. Components considered as a single isolated component will result in a test restart for the individual component.

8.13.19. Disassemble and Re-Pack for Shipment

Once full system staging has completed successfully, the contractor shall disassemble equipment and prepare for shipping to the PSAP or training center for installation. The contractor shall ensure that equipment shall not arrive at the PSAP or training center any sooner than seventy-two (72) hours prior to commencement of installation work.

The contractor shall note any necessary changes identified during the initial site visit, and such changes require approval by State 911 Department. The contractor shall provide the State 911 Department with a copy of the notes from the initial site visit before any cutover can commence on the identified changes.

The State 911 Department representative shall conduct periodic site visits to check on the status of the cutover. The PSAP administrator or designee shall be available during the cutover to address any site-specific questions from the contractors.

Pre-Cutover Testing

The contractor shall perform a pre-cutover test prior to the cutover date to ensure that all of the system features and functions are performing in accordance with the pre-cutover test portion of the Functionality Checklist. The contractor shall successfully complete the pre-cutover testing at least forty-eight (48) hours prior to the scheduled cutover date. If said testing is not successfully completed, the State 911 Department shall be notified and the State 911 Department shall determine if the cutover date requires rescheduling.

If any section of the pre-cutover test is not successfully completed, the planned cutover may be postponed at the election of the State 911 Department upon notice to the contractor. If postponed, the contractor shall be required to reschedule the cutover date to another date approved by the State 911 Department.

Cutover Testing

The contractor shall successfully complete cutover testing on the planned cutover date based on an agreed upon functionality checklist in order for the cutover to take place. The contractor shall document its activities in connection with the checklist, including pass/fail metrics, measurement criteria used to determine pass/fail metrics, and the results. The contractor and the State 911 Department shall jointly conduct the cutover day testing.

Post-Cutover Testing

After the cutover is completed, a post-cutover test shall be conducted to ensure that all systems and functions are performing based on an agreed upon post-cutover checklist. The contractor shall document its activities in connection with the checklist, including pass/fail metrics, measurement criteria used to determine pass/fail metrics, and results.

If any section of the post-cutover test is not successfully completed, the State 911 Department may halt the testing. The contractor shall be required to immediately repair the problem. Post-cutover testing shall re-commence only at the direction of the State 911 Department's order following notification from the contractor that the problem has been repaired. If the problem(s) cannot be repaired within four (4) hours of the start of the post-cutover testing, the State 911 Department may halt the cutover until the problem can be repaired satisfactorily. In the event of a post-cutover test failure, the State 911 Department shall determine whether additional testing is required. The contractor shall provide any additional testing required by the State 911 Department.

GDIT will comply with the RFR specification.

Once staging is completed, GDIT will break down the staged equipment suite and prepare it for shipping to its final installation site. The staging breakdown/packing effort encompasses:

- Collection of component serial numbers for input to the serial number spreadsheet for tracking purposes.
- Power down and physical de-installation of components and cabling.

- Packaging of system components. Packing slips will be created that contain part number, description, quantity, and serial number (if applicable). Slips will also identify the functional element and installation location. All packing lists will be provided to the State 911 Department.

GDIT will ensure that equipment will not arrive at the PSAP or training center any sooner than seventy-two (72) hours prior to commencement of installation work.

Once on site, the GDIT will perform physical installation and power-up of system components at the PSAP or training center. The next step after physical installation and power-up involves successful completion of acceptance tests that are a prerequisite for system cutover. Pre-cutover tests will be documented in its section of the Functionality Checklist for the PSAP or training center site. These tests ensure that all system features and functions are performing and will include at a minimum:

- 9-1-1 telecommunicator logins
- Autodials and other system features for the hosted CPE application
- Network integration for Syslog, NTP, DNS, etc.
- Management functionality
- 9-1-1 call routing
- Software/hardware redundancy tests

Pre-cutover testing will be successfully completed at least 48 hours prior to the scheduled cutover event. If testing is not completed within the specified timeline, GDIT will notify the State 911 Department. GDIT understands that the State 911 Department will then determine if the cutover date requires rescheduling. If postponed, GDIT will coordinate with the State 911 Department to reschedule the cutover to another date.

As part of system cutover, GDIT will successfully complete testing to validate successful transition of the PSAP or training center to the new system architecture. Testing will be based on an agreed-upon functionality checklist and will be jointly conducted by GDIT and the State 911 Department. The checklist will contain test procedures, pass/fail metrics, measurement criteria, and a section to document the actual test results.

Post-cutover testing will be performed to ensure that all transitioned systems are completely functional. Testing will be based on a pre-approved post-cutover checklist and will include, at a minimum:

- Call routing for all applicable 9-1-1 payloads
- Integration with local CAD and recording systems

The checklist will contain test procedures, pass/fail metrics, measurement criteria, and a section to document the actual test results. GDIT understands that the State 911 Department may halt testing should any portion of the post-cutover verification not be successful. GDIT will immediately address and resolve any issues to allow post-cutover testing to recommence at the direction of the State 911 Department.

A four-hour window will be employed for troubleshooting and resolving post-cutover issues. GDIT understands that the State 911 Department may halt cutover should troubleshooting efforts

take longer than the prescribed four hours. The cutover event will not move forward until the problem is resolved to the satisfaction of the State 911 Department. If required by the State 911 Department, GDIT will perform additional post-cutover testing to properly demonstrate resolution to identified post-cutover test failures.

8.13.20. Waste Disposal

The contractor shall be responsible for the removal of any and all packing or other materials associated with the delivery and/or installation of any and all system components at the PSAPs, training centers, and data centers.

GDIT will comply with the RFR specification.

At the end of every workday, GDIT installation teams at each site will:

- Sweep work areas clean to remove scrap material
- Remove and dispose of trash from the premises

At the end of the project, excess unused material will either be turned over to the State 911 Department, if so desired, or completely removed from site facilities.

8.14. ACCEPTANCE OR REJECTION PROCESS

The contractor shall submit the required deliverables specified in this RFR to the State 911 Department for approval and acceptance. The State 911 Department shall review work product for each of the deliverables and evaluate whether each deliverable has clearly met in all material respects the criteria established in this Agreement. Once reviewed and favorably evaluated, the deliverables will be deemed acceptable.

Acceptance of the work of the contractor shall not preclude the State 911 Department from requiring strict compliance with the contract, in that the contractor shall complete or correct upon discovery any faulty, incomplete, or incorrect work not discovered at the time of acceptance.

GDIT will comply with the RFR specification.

GDIT will submit all RFR-specified deliverables to the State 911 Department for approval and acceptance. GDIT understands the review and acceptance process that the State 911 Department will employ for contract deliverables. GDIT will complete or correct upon discovery any faulty, incomplete, or incorrect work not discovered at the time of acceptance.

8.14.1. Acceptance or Rejection of Site Cutovers

After the PSAP or training center has operated for fifteen (15) calendar days at full functionality with the new CPE, the contractor shall provide the State 911 Department with a Cutover Acceptance Report that shall contain all trouble tickets created since the cutover and additional performance metrics as agreed to by the parties. The State 911 Department shall verify the level of functionality by reviewing the trouble tickets and performance metrics and conducting a site inspection within fifteen (15) days after it receives the Cutover Acceptance Report that contains the trouble tickets and performance metrics. Once the State 911 Department performs this inspection, if it is satisfied with the performance level of the PSAP, it will sign the Cutover Acceptance Report. The Site Acceptance Date shall be the date of execution of the Cutover Acceptance Report by the State 911 Department. The contractor shall remove the legacy 911 CPE from the PSAP within ten (10) business days of the Site Acceptance Date. The contractor shall notify the State 911 Department upon completion of said work and the 911 Department will inspect the site.

GDIT will comply with the RFR specification.

GDIT will provide the State 911 Department with a Cutover Acceptance Report to be submitted after the PSAP or training center has operated for fifteen (15) calendar days at full functionality. The Cutover Acceptance Report will contain:

- Report header/signature page
- Trouble Ticket Log
- Trouble Tickets
- Performance metric documentation as agreed to between the State 911 Department and GDIT

We understand that:

- The State 911 Department will conduct a site inspection within fifteen (15) days of receipt of the Acceptance Report for the purpose of determining the level of functionality for the transitioned PSAP or training center.
- Upon satisfactory inspection, the State 911 Department will sign the Acceptance Report. The date of the signature constitutes the acceptance date for the transitioned site.

GDIT will remove all legacy 9-1-1 CPE from the transitioned PSAP within ten (10) business days of the site acceptance date. GDIT will notify the State 911 Department upon completion of the de-installation effort and will work with the Department to address any issues resulting from its inspection of the equipment de-installation.

8.14.1.1. Site Cutover Acceptance Package

Following acceptance of the cutover of a PSAP or training center by the State 911 Department, the contractor shall submit the following information to the State 911 Department for each such accepted PSAP or training center:

a) CPE inventory, including a complete list of installed equipment that identifies, at a minimum, manufacturer name, serial numbers, and part numbers, for the installed equipment;

b) Sales configurations and associated change control request orders;

c) Software Inventory Document;

d) Cutover Acceptance Report;

e) Pre-cutover test checklist;

f) Post-cutover test checklist; and

g) Any other information as mutually agreed to by the parties.

GDIT will comply with the RFR specification.

Following State 911 Department cutover acceptance for a PSAP or training center, GDIT will submit a Site Cutover Acceptance Package that includes the following:

- Inventory management spreadsheet with the following information at a minimum:
  - Part number, description, and OEM
  - Serial numbers
  - Installation location data to include physical address, equipment room designation, and site POC
  - Installation dates
  - Warranty start and end dates

— Spares inventory (if spares are maintained locally)

- Spec-book that documents site-specific configurations, software inventory, network information (i.e., IP address, VLANs, etc.), and change control request orders
- Cutover Acceptance Report including trouble ticket log, actual trouble tickets, and agreed-to performance metrics
- Pre-cutover and post-cutover test checklists/results
- Other information/data as agreed to between the State 911 Department and GDIT

GDIT will the Site Cutover Acceptance Package no later than seven business days after cutover acceptance by the State 911 Department.

8.14.2. Acceptance of Other Deliverables

Within ten (10) business days of receipt of each Deliverable (other than for PSAP or training centers), the State 911 Department will notify contractor, in writing, of the acceptance or rejection of said Deliverable using the acceptance criteria specified in this Section 8.14.2 and associated with the Task or Deliverable specifications. A form signed by State 911 Department shall indicate acceptance. The contractor shall acknowledge receipt of acceptance forms in writing. Any rejection shall include a written description of the defects of the deliverable. If State 911 Department does not respond to the submission of the Deliverable, within five (5) business days of the State 911 Department's receipt of each Deliverable, the contractor shall provide a reminder notice to the State 911 Department. If the State 911 Department fails to reject a Deliverable within five (5) business days after State 911 Department's receipt of the reminder notice, the Task or Deliverable is deemed accepted.

If the State 911 Department rejects a Deliverable, the contractor shall, upon receipt of such rejection, act diligently to correct the specified defects and deliver an updated version of the Deliverable. The State 911 Department shall then have an additional five (5) business days from receipt of the updated Deliverable to notify the contractor, in writing, of the acceptance or rejection of the updated Deliverable. Any such rejections shall include a description of the way in which the updated Deliverable fails to correct the previously reported deficiency.

Following any acceptance of a Deliverable which requires additional work to be entirely compliant with the pertinent specifications, and until the next delivery, the contractor shall use reasonable efforts to provide a prompt correction or workaround.

GDIT will comply with the RFR specification.

GDIT understands the acceptance/rejection criteria described in RFR Paragraph 8.14.2. GDIT will acknowledge receipt of acceptance in writing to the State 911 Department. GDIT will update any rejected deliverable to incorporate comments provided by the State 911 Department. Updated deliverables will be resubmitted for State 911 Department review no later than seven business days from receipt of comments.

8.14.3. De-Installation of Legacy CPE

As authorized by the State 911 Department in connection with site cutovers and otherwise at the request of the State 911 Department, the contractor shall de-install any and all legacy CPE, including without limitation, servers, cabling workstations, interfaces, etc., to be stored in a location on-site at the PSAP or such other location to be designated by the State 911 Department. All such work shall be performed under oversight by the State 911 Department.

GDIT will comply with the RFR specification.

GDIT will remove all legacy CPE equipment at each PSAP that is replaced as a result of the migration to the new NG9-1-1 architecture as authorized by the State 911 Department. De-

installation effort will be performed in connection with individual site cutovers and/or at the request of the State 911 Department. De-installation by GDIT will be a turn-key effort to include all replaced hardware (server(s)/workstation(s)), cabling, and legacy dispatch/administrative communication/Selective Router interfaces. De-installed equipment will be stored on-site at the PSAP or at a location designated by the State 911 Department.

8.14.4. Retainage

The State 911 Department will retain ten (10) percent of the total amount due to the contractor on each invoice for each Deliverable in Milestone Categories 1, 2, and 3. The State 911 Department will retain these amounts whether or not the contractor's performance is timely or the deliverable has met all of the State 911 Department's requirements for acceptance. The State 911 Department will release this ten (10) percent to the contractor if Milestone 4 commences on or before February 1, 2015. If Milestone 4 does not commence on or before February 1, 2015, the amount retained shall be forfeited to the Commonwealth, unless the State 911 Department elects, in its sole discretion, to waive such forfeiture.

In addition, the State 911 Department will retain five (5) percent of the total amount due to the contractor on each invoice for each Deliverable in Milestone 4. The State 911 Department will retain these amounts whether or not the contractor's performance is timely or the deliverable has met all of the State 911 Department's requirements for acceptance. If the contractor meets the PSAP deployment installation deadlines set forth in Attachment L- Project Schedule, Milestone, and Deliverables, to be assessed and evaluated for each Deliverable Due Date of the Milestone 4 deployment period, the State Department will release fifty (50) percent of this five (5) percent to the contractor. If the contractor fails to meet the Deliverable Due Dates set forth in Milestone 4 of Attachment L- Project Schedule, Milestone, and Deliverables, to be assessed and evaluated for each Deliverable Due Date for the duration of Milestone 4, the amounts retained for the Deliverable Due Date shall be forfeited to the Commonwealth, unless the State 911 Department elects, in its sole discretion, to waive such forfeiture. If the contractor fails to complete all Milestone 4 Deliverables on or before June 30, 2016, all amounts retained for Milestone 4 shall be forfeited to the Commonwealth, unless the State 911 Department elects, in its sole discretion, to waive such forfeiture. The State 911 Department will retain fifty (50) percent of the retainage amounts referenced in this paragraph until the expiration of the one (1) year warranty period for the last PSAP deployed.

GDIT will comply with the RFR specification.

8.15. PSAP AND DATA CENTER MOVES

As requested by the State 911 Department, the contractor shall provide all necessary services to relocate or move existing PSAP and/or data center CPE to a new location within the existing site or to a new site while minimizing service interruptions of such PSAP or data center. Services shall include project management, scheduling, and coordination of appropriate resources. The contractor shall utilize a step-by-step conversion checklist for each PSAP or data center relocation or move. The contractor shall submit detailed cost estimates for moves to the State 911 Department on a case by case basis. The cost estimate shall set forth in detail each component of the estimated cost to the satisfaction of the State 911 Department. The cost estimate shall utilize a unique identifier for each such detailed cost estimate. The contractor may be required to install electrical components, network cabling, and any common components that do not require special configuration at the new location prior to moving CPE in order to reduce PSAP or data center service interruption. The contractor shall also coordinate with EOPSS on network circuit moves as needed for Commonwealth assets.

GDIT will comply with the RFR specification.

As requested, GDIT will provide turn-key services to relocate or move existing PSAP and/or data center CPE to a new location within an existing site or to a new site. GDIT's implementation approach will minimize service disruption to the affected PSAP or data center. Services will include project management, scheduling, and coordination of all technical resources necessary to successfully accomplish the relocation. GDIT will use a step-by-step conversion checklist for each move. The checklist will cover all steps from site survey through final acceptance to accomplish the relocation.

GDIT will submit detailed cost estimates for moves to the State 911 Department on a case-by-case basis. Cost estimates will be detailed in nature providing a breakdown for each component of the proposed move. Breakdowns will be sufficiently detailed to ensure State 911 Department satisfaction. A unique identifier will be used for estimate submitted.

GDIT understands that electrical infrastructure, network cabling, and/or additional hardware/software may be necessary to minimize service disruption. These costs, if necessary, will be reflected in the detailed cost estimate. GDIT will coordinate with EOPSS on network circuit moves, as required, for Commonwealth assets.

8.16. PSAP AND DATA CENTER EQUIPMENT INVENTORY

The contractor shall provide a list of any and all newly installed components and the associated serial numbers of PSAP and data center equipment to the State 911 Department. The contractor shall maintain for each PSAP and data center, a serial number database and shall promptly update such database whenever a hardware component is changed or new PSAP CPE or data center equipment is added. An electronic copy of this database in an Excel or Access format shall be provided to the State 911 Department annually and as otherwise requested by the State 911 Department. For the duration of the contract, the contractor shall maintain as current and supply to the State 911 Department annually and upon request an As Built diagram, including CPE and data center configuration and cabling details.

GDIT will comply with the RFR specification.

GDIT's inventory management database will include serial number listings by location for all newly installed NG9-1-1 hardware. GDIT's support organization will be responsible for database updates when required by warranty action or equipment addition. GDIT will provide a copy of the database in Microsoft Office format (Excel or Access format) annually or as requested by the State 911 Department. GDIT will also provide annually or upon request, an as-built diagram to include CPE and data center configuration and cabling details.

8.17. Circuit ID INVENTORY

The contractor shall provide a list of all circuit IDs for each connection and shall identify where the circuit(s) is connected, including the a and z end locations. The contractor shall maintain an inventory of all circuit IDs, and the contractor shall promptly update this database whenever a circuit is changed, moved, or added. The contractor shall promptly notify the State 911 Department of all changes in circuit. An electronic copy of this database in an Excel or Access format shall be provided to the State 911 Department annually and as otherwise requested by the State 911 Department.

GDIT will comply with the RFR specification.

GDIT will maintain a circuit ID inventory for all data center to data center and data center to PSAP connections. Data documented for each circuit will include:

- Unique circuit ID
- Circuit type and bandwidth
- Signaling protocol(s)
- Functionality provided by the circuit
- Circuit provider to include POC data
- Termination data for each end of the circuit to include:
  - Room number, rack location, patch panel designation, and port assignments as applicable

  - Physical address
  - Site POC
- Interconnection points including any circuit termination equipment details such as type, model, port number, etc. will be tracked.

GDIT's support organization will be tasked with maintaining the circuit inventory. As new circuits are added or existing circuits changed, the inventory will be updated to reflect the new as-built configuration. GDIT will notify the State 911 Department when any change in circuit data occurs. GDIT will provide a copy of the circuit inventory in Microsoft Office format (Excel or Access format) annually or as requested by the State 911 Department.

8.18. INVENTORY MANAGEMENT

The contractor shall maintain an inventory management system and database. Bidders shall describe the inventory management system in detail. The inventory management system and database shall provide the State 911 Department with access to inventory management reports, and shall provide the State 911 Department with the ability to create ad hoc reports.

GDIT will comply with the RFR specification.

GDIT has developed and will maintain a configuration and asset management database system that will be customized and implemented into the MA NG9-1-1 environment. The configuration and asset management and enterprise reporting system consists of a Microsoft Access front-end coupled to a Microsoft SQL Server database back-end. A series of human interface menus and screens provide the Commonwealth system administrators with the ability to manage all logistical aspects the project.

This system has the capability of providing hardware and software inventories, auditing, developing equipment hierarchies and logical groups, customizing reporting, tracking movements and changes, establishing a baseline, and future baselines resulting from approved system modifications. System reporting uses Microsoft SQL Server Reporting Services-based reports capable of supporting development of customized ad hoc reports or standardized reports as required by the Commonwealth.

All equipment will be labeled with a bar code label identifier and, to the greatest extent possible, will be electronically entered into the database – eliminating the possibility of human error. Once the initial set of data is loaded into the database, the data will be normalized to ensure identical items are identified with a standardized nomenclature.

Upon delivery of the system, GDIT will have barcoded each of the equipment elements provided and completed as-built documentation for each of the racks, workstations, and network elements. This data will be placed within our inventory database system and be submitted to the State 911 Department and during the warranty period will be updated by GDIT.

GDIT will maintain the inventory management system and database for the NG9-1-1 project.

GDIT's support organization will be charged with the responsibility for keeping the database current during the course of the contract. Any changes resulting from corrective actions taken during the support will be incorporated into the database to ensure it accurately reflects the

current as-built configuration. The system will provide the State 911 Department with access to inventory management reports as well as the ability to create as hoc reports.

8.19. ELECTRICAL, WIRING, AND CABLE

The contractor shall provide and maintain all electrical, wiring, and cable services for the system. The State 911 Department has a preference for the reuse of existing wiring, cabling, and HBCU, if compatible with the system.

GDIT will comply with the RFR specification.

GDIT will provide and maintain all electrical, wiring, and cabling services for the system. GDIT's proposed solution will reuse existing wiring, cabling, and HBCU to the maximum extent practical.

8.19.1. Electrical

The contractor shall provide and maintain all electrical services for the system and shall provide such electrical services as follows:

- *Supply and install where needed and otherwise maintain existing complete electrical power distribution system for all equipment supplied;*
- *Provide adequate surge protection, grounding and lightning suppression devices to protect equipment from unnecessary interruption; and*
- *Provide and maintain a thirty (30) minute uninterruptible power supply for all equipment supplied at the PSAPs and for data centers and for all DLRs. A hard bypass unit for maintenance/equipment failure is required. Following contract award, the parties shall, by mutual agreement, determine the means and manner of installing the uninterruptible power supply so as to ensure that there is no interruption for the PSAP or data center. Bidders shall describe in detail the UPS, including the size and weight of the UPS.*

The contractor shall ensure that all electrical services performed by the contractor or its subcontractors under the contract, and any renewal thereof, shall be performed by appropriately licensed electricians. The contractor shall ensure that the contractor or its subcontractors shall obtain any and all necessary permits for electrical services performed by the contractor or its subcontractors under the contract, and any renewal thereof, and shall provide copies of such permits to the State 911 Department upon request. The State 911 Department reserves the right to contract with its own electrician for such work if to do so would result in the best value in fulfilling the contract, or any renewal thereof.

GDIT will comply with the RFR specification.

Where needed, GDIT will supply and maintain all electrical services for the NG9-1-1 architecture at each location. This includes:

- Protected 110 infrastructure at the non-Commonwealth data center
- Managed Power Distribution Units (PDUs) installed at the PSAPs
- UPS systems (providing 30 minutes of up time) installed at the PSAPs. See Table 30 for model information.

PDUs and UPS systems furnished and installed by GDIT will include surge suppression capability to protect equipment. New antennas installed by GDIT will include lightning arrestors connected to a copper clad ground rod in accordance with the National Electrical Code (NEC).

GDIT will furnish and install an APC SmartUPS at the PSAP locations to provide 30 minutes of runtime for the back office equipment and 9-1-1 call taker hardware and for all existing or new DLRs. The proposed UPS includes a hard bypass unit for maintenance and extended battery module to provide the required backup power runtime. GDIT will coordinate the implementation

approach for the UPS equipment at each site with the State 911 Department. UPS installation will not affect service for the PSAP locations.

Any required electrical services will be performed by a licensed electrician. GDIT will obtain any and all permits as needed for electrical services. Permit costs will be provided to the State 911 Department upon request. GDIT understands that the State 911 Department reserves the right to contract with its own electrician to provide required electrical services.

8.19.1.1. Electrical Standards

All devices shall be provided with any and all necessary connecting cords and cables conforming to National Electrical Manufacturers Association (NEMA) codes.

GDIT will comply with the RFR specification.

All AC-powered hardware proposed for the NG9-1-1 architecture will conform to National Electrical Manufacturers Association (NEMA) codes.

8.19.1.2. Surge Protection/Surge Suppression

The system shall correctly specify surge and lightning protection for all connections to AC power as well as to communications facilities such as plain old telephone service, 911 trunks, T1/DS1, wireless antennas, etc.

GDIT will comply with the RFR specification.

All PDUs and UPS proposed by GDIT include surge suppression functionality as a baseline requirement. New antennas installed by GDIT will include lightning arrestors connected to a copper clad ground rod in accordance with the National Electrical Code (NEC).

With respect to existing Commonwealth communication facilities, electrical panels, and antennas, it is assumed that they are properly grounded. GDIT will document any grounding deficiencies noted during the site survey conducted for any of the Commonwealth locations where equipment is planned. These details will be included in the corresponding site survey report.

8.19.2. Wiring and Cabling

8.19.2.1. System Cabling

This project will require the cooperation of the State 911 Department, the Commonwealth's IT Department and the contractor. The contractor shall provide all necessary embedded and visible interconnect cabling necessary for system operation, including all peripheral devices located within the data centers and PSAPs, connecting remote workstations with the central servers. The LAN/WAN system requirements shall be included in the RFR response. Bidders shall indicate preferred communications devices and configuration within their response, based upon proven experience with this equipment.

All interface connections between communications and peripheral device cabling and visible cables shall use standard EIA connectors secured by wall plates where exposed.

Care shall be exercised in wiring to avoid damage to existing wiring and new and existing equipment. All wiring and connectors shall be installed in strict adherence to standard communication installation practices and all applicable federal, state, and local codes.

All cables, regardless of length, shall be clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends. Marking codes shall correspond to recognized standards and specifications and be consistent throughout the project. Such markings shall become integral to the overall as-built detail. All cabling shall be neatly laced, dressed, and/or adequately supported. Cable shall be plenum rated where required by local building or fire codes.

No splices will be allowed in system wiring other than at approved designated locations, and with approved devices.

The equipment installation required by this RFR includes the following described items as well as other hardware, software, and procedures as may be needed to ensure a completed installation which is in accordance with the standards of good engineering practice and all building codes and ordinances in effect at the sites delineated in this RFR.

Wiring of 120-volt AC circuits normally associated with conventional buildings shall be provided by the State 911 Department at the data centers and PSAPs and other Commonwealth facilities as required. Wiring required for connecting the equipment to the power outlets or any special wiring shall be the responsibility of the contractor.

The contractor shall install the equipment and connect the units to commercial/emergency AC power and uninterruptible power sources. The contractor shall connect Commonwealth-furnished equipment to the contractor-supplied equipment and install bonding and grounding conductors where needed.

The proposal price shall include installation hardware, brackets, braces, fasteners of all kinds, wiring, ancillary devices, procedures, and services required to install and/or interface components to provide a complete operating system that fulfills the requirements of this RFR.

The contractor shall adhere to FCC and all local codes and ordinances in all matters pertaining to the work.

Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms shall be installed in accordance with national standards and national and local codes. Minimum standards used in the installations shall include, but are not limited to, the following:

ANSI/TIA/EIA-568 Commercial Building Telecommunications Wiring Standard;

ANSI/TIA/EIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces;

ANSI/TIA/EIA-606 Administration Standard for the Telecommunications Infrastructure of Commercial Buildings;

ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunications;

Building Industry Consulting Service International, Telecommunications Distribution Methods Manual;

National Electrical Code (NFPA-70);

FCC Rules and Regulations, Parts 68 and 15; and

Applicable grounding standards.

All equipment and component parts installed shall be new, shall meet the requirements of this specification, and shall be in operable condition at the time of delivery.

The installation work shall be approved by the State 911 Department prior to commencement of a particular phase of work on a site-by-site basis. The contractor shall provide descriptions and layout drawings showing the proposed installations at each site at least fourteen (14) days prior to beginning work at that site. No work shall commence without written approval from the Department.

The contractor shall supply all cabinets in the data centers (except that, if Commonwealth data centers are utilized, the Commonwealth will supply the cabinets). Mounting for equipment or any other data communications equipment (i.e., modems, routers, etc.) requiring assisted installation shall be accomplished by cabinet mounting. The cabinets may be free-standing or wall mounted depending upon space requirements. Bidders shall describe the recommended method for cabinet mounting, and shall provide an option for any other recommended method. The State 911 Department shall select the preferred method of cabinet mounting following contract award. Cabinets shall in no event no exceed eighty-four (84) inches in height. The response shall describe in detail the space requirements and dimensions of all equipment, including without limitation, the size of cabinets, tables, stands, and consoles, for the system.

Bidders shall provide all necessary cabinets, tables, stands, or other required mounting facilities for the system (with the exception of the Commonwealth data centers, since the Commonwealth will supply the cabinets and mounting facilities for the Commonwealth data centers if utilized), consoles, and communications and/or network equipment consistent with their proposed configuration(s).

Bidders shall inform themselves fully as to all facilities for delivering, storing, placing, handling, and disposing of materials. All aspects of the installation shall be planned and executed in a professional manner. The contractor shall coordinate access to the sites with the State 911 Department.

The costs for wiring and cabling shall be on a time and materials basis.

GDIT will comply with the RFR specification.

GDIT's turn-key solution includes all required embedded and visible cabling to interconnect NG9-1-1 subsystems to one another. Cabling will use standard Electronic Industries Alliance (EIA) connectors. Where applicable, cables will be terminated using wall plates. Paths for new system cabling will be determined during the surveys conducted at each site. Existing paths will be re-used to the maximum extent practical. GDIT installers will exercise care when installing new cabling in the same space as existing cabling to avoid damage and service interruptions. All wiring and connectors will be installed in strict adherence to standard communication installation practices as well as any applicable federal, state, and/or local codes. GDIT will employ the same methodology for cable identification as is used for DoD installations. Cable labels will include the following information:

- Cable number identification: The identifier is an alpha-numeric combination that consists of:
  - An identification of the cable type. For example, telecommunication cables, such as Cat 5, will use "TE" to identify telecommunication. AC power cords will use "ACP" as the identifier.
  - A four-digit number.
- Local termination information: This includes component identification and port information.
- Far end termination information: This includes component identification and port information.

Labels will be affixed to cabling using P-145 tags and waxed lacing cord. Cable label information will be included in design drawings related to system cabling. All new cabling will be dressed using lacing cord or Velcro straps. Plenum-rated spaces will be identified during the site surveys. New system cabling installed in these spaces will be plenum-rated or housed in plenum-rated innerducts. All new cabling will be connectorized. The only splices that may be necessary would be for ground cabling where an H-tap is used to reduce the size of the ground cabling that terminates to the frame of new equipment racks.

GDIT will comply with all stated national and local codes and ordinances as well as OEM-recommended guidelines for deployment of the NG9-1-1 architecture. GDIT's proposed solution is turn-key and includes all necessary hardware, software, cabling (signal/power/ground), ancillary material (e.g., brackets, lugs, etc.), and services to provide a fully functional integrated solution for the Commonwealth of Massachusetts. This includes interconnections and integration effort between Commonwealth-furnished systems and GDIT-furnished systems. Design documentation will include all drawings and technical descriptions necessary to fully convey the NG9-1-1 architecture for each location. Delivery of this documentation will occur no later than 14 days prior to the beginning of work at a particular site. Installation activity will not commence without written approval from the State 911 Department.

GDIT's proposed solution includes equipment cabinets for its proposed footprint at the data centers. GDIT understands that the Commonwealth will supply the cabinets should a Commonwealth data center be used. GDIT's recommended method for installing new cabinets at the data centers involves mounting the cabinets to the concrete subfloor using threaded rods and appropriate fastening hardware. Where possible, racks will also be top-mounted to an existing/new overhead cable ladder. All proposed equipment for the data center will be rack-mounted within the equipment cabinets.

GDIT will use a combination of half and full cabinets for the PSAPs. The size of the PSAP determines which will be used. The equipment suite for the smaller PSAPs (2- position through 5-position) can be accommodated in a half cabinet. The larger sites (6-position and above) will require a full cabinet for the back office hardware. Table 30 provides equipment details and dimensions for the half and full equipment suite planned for the back-office at the small and large PSAP locations. Figure 85, Figure 86, and Figure 87 provide preliminary equipment elevations for the large and small PSAP sites.

Table 30. Equipment Suite Description for Back Office PSAPs

Description	Vendor	Part Number	Dimension (HxWxD) inches	Remarks
Small PSAP Sites				
Equipment Cabinet	Great Lakes	4801E-2432	48 x 24 x 32	24 rack-mount units available
Network Router	Cisco	CISCO1921-SEC/K9	1.75 x 17.5 x 15.1	1–4 T1s back to Data Center depending on size of site
Layer 2 Network Switch – 24 Ports	Cisco	WS-C3650-24	1.75 x 17.5 x 15.1	Twenty-four (24) 10/100/1000 ports
IP Network Monitoring	Acme Packet	HP DL160G8	1.7 x 17.1 x 27.5	Palladion Network Probe Server residing on HP server
NTP Server	Spectracom	Netclock 9483	1.72 x 16.75 x 14	
CAD Interface Module	Lantronix	UDS1100	0.9 x 3.5 x 2.5	
UPS	APC	SMX3000RMLV2U	3.4 x 17.0 x 26.3	84.6 lb.
UPS Extended Battery Module	APC	SMX120RMBP2U	3.4 x 17.0 x 26.3	82.1 lb.
UPS Maintenance Bypass	APC	SBP3000RM	3.5 x 17.0 x 3	9.8 lb.
Large PSAP Sites				
Equipment Cabinet	Great Lakes	NG911GL84OES-KIT	84 x 24 x 42	44 rack-mount units available
Network Router	Cisco	CISCO1921-SEC/K9	1.75 x 17.5 x 15.1	5 T1s and up back to Data Center depending on size of site
Edge Router	Cisco	ISR4451-X-SEC/K9	3.5 x 17.25 x 18.7	For 21-, 22-, and 45-position PSAP sites connecting back to the Data Centers
Layer 2 Network Switch – 24 Ports	Cisco	WS-C3650-24	1.75 x 17.5 x 15.1	Twenty-four (24) 10/100/1000 ports
Layer 2 Network Switch – 48 Ports	Cisco	WS-C3650-48	1.75 x 17.5 x 15.1	Forty-eight (48) 10/100/1000 ports
IP Network Monitoring	Acme Packet	HP DL160G8	1.7 x 17.1 x 27.5	Palladion Network Probe

Description	Vendor	Part Number	Dimension (HxWxD) inches	Remarks
				Server residing on HP server
NTP Server	Spectracom	Netclock 9483	1.72 x 16.75 x 14	
CAD Interface Module	Lantronix	UDS1100	0.9 x 3.5 x 2.5	
UPS	APC	SMX3000RMLV2U	3.4 x 17.0 x 26.3	84.6 lb.
UPS Extended Battery Module	APC	SMX120RMBP2U	3.4 x 17.0 x 26.3	82.1 lb.
UPS Maintenance Bypass	APC	SBP3000RM	3.5 x 17.0 x 3	9.8 lb.

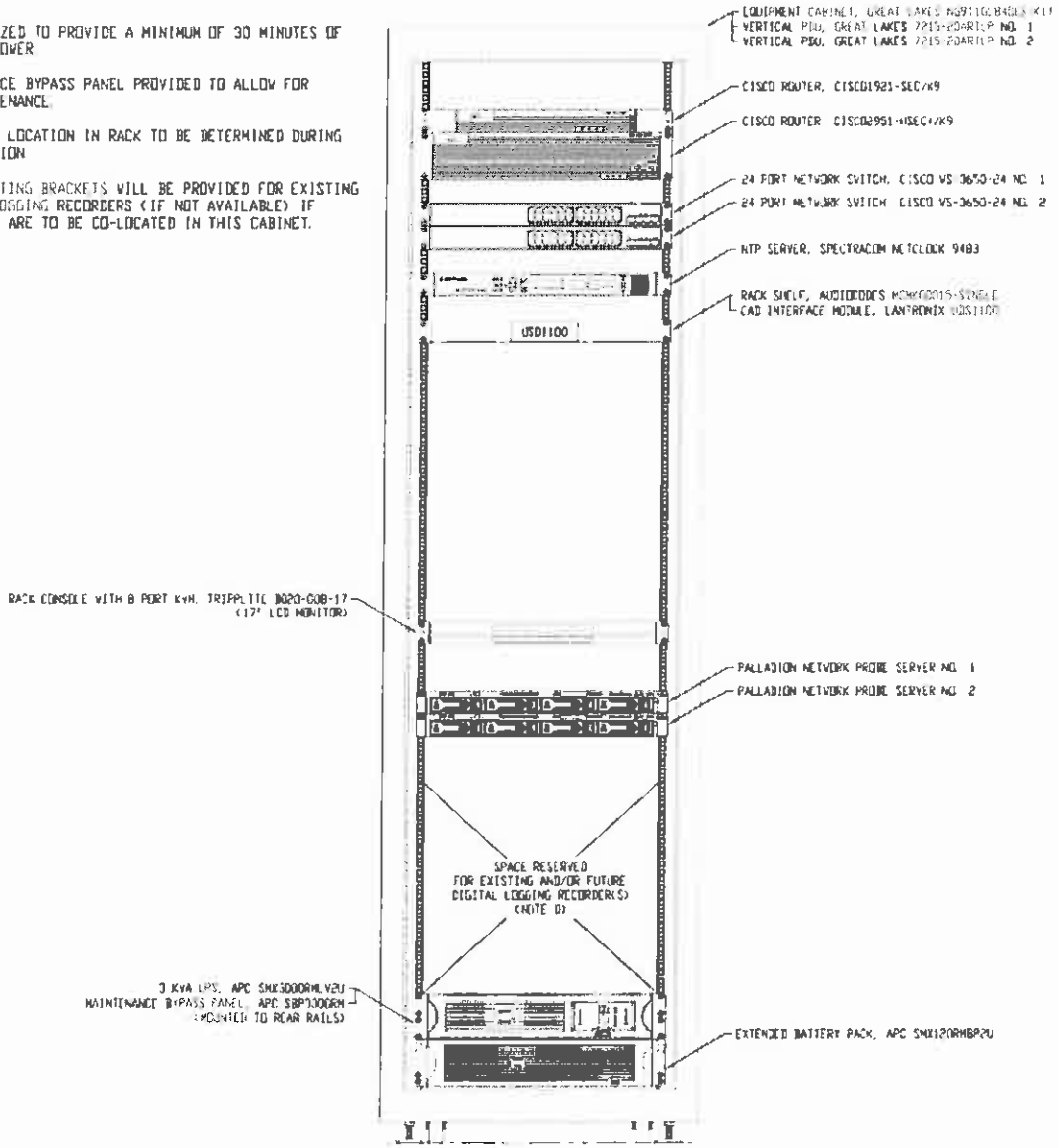
NOTES:

A. UPS IS SIZED TO PROVIDE A MINIMUM OF 30 MINUTES OF BACK-UP POWER

B. MAINTENANCE BYPASS PANEL PROVIDED TO ALLOW FOR UPS MAINTENANCE.

C. EQUIPMENT LOCATION IN RACK TO BE DETERMINED DURING INSTALLATION

D. RACK MOUNTING BRACKETS WILL BE PROVIDED FOR EXISTING DIGITAL LOGGING RECORDERS (IF NOT AVAILABLE) IF RECORDERS ARE TO BE CO-LOCATED IN THIS CABINET.



SMALL PSAP CABINET
ONE 30A CIRCUIT REQUIRED FOR EQUIPMENT CONNECTED TO UPS
(SIX (6) TO EIGHT (8) POSITION PSAPS)

SMALL PSAP (6 TO 8 POS) EQUIPMENT SCHEDULE				
RU	ITEM	QUANTITY	VOLTS	WATTS
1	CISCO1921-SEC/K9 ROUTER	1	110	150
2	CISCO2951-HSEC+/K9	1	110	60
1	24 PORT CISCO NETWORK SWITCH	2	110	150
1	NTP SPECTRACOM NETCLOCK 9483	1	110	40
0	LANTRONIX CAD INTERFACE MODULE	1	110	1.5
1	TRIPPLITE RACK CONSOLE	1	110	24
1	PALLADION NETWORK PROBE SERVER	2	110	400
2	APC 3KVA UPS (NOTE A)	1	110	50
2	APC EXTENDED BATTERY PACK (NOTE A)	1	110	N/A

ONE RU IS 1.75"H

Figure 85. Preliminary Equipment Elevation – Small-Medium PSAP (6–8 Positions)

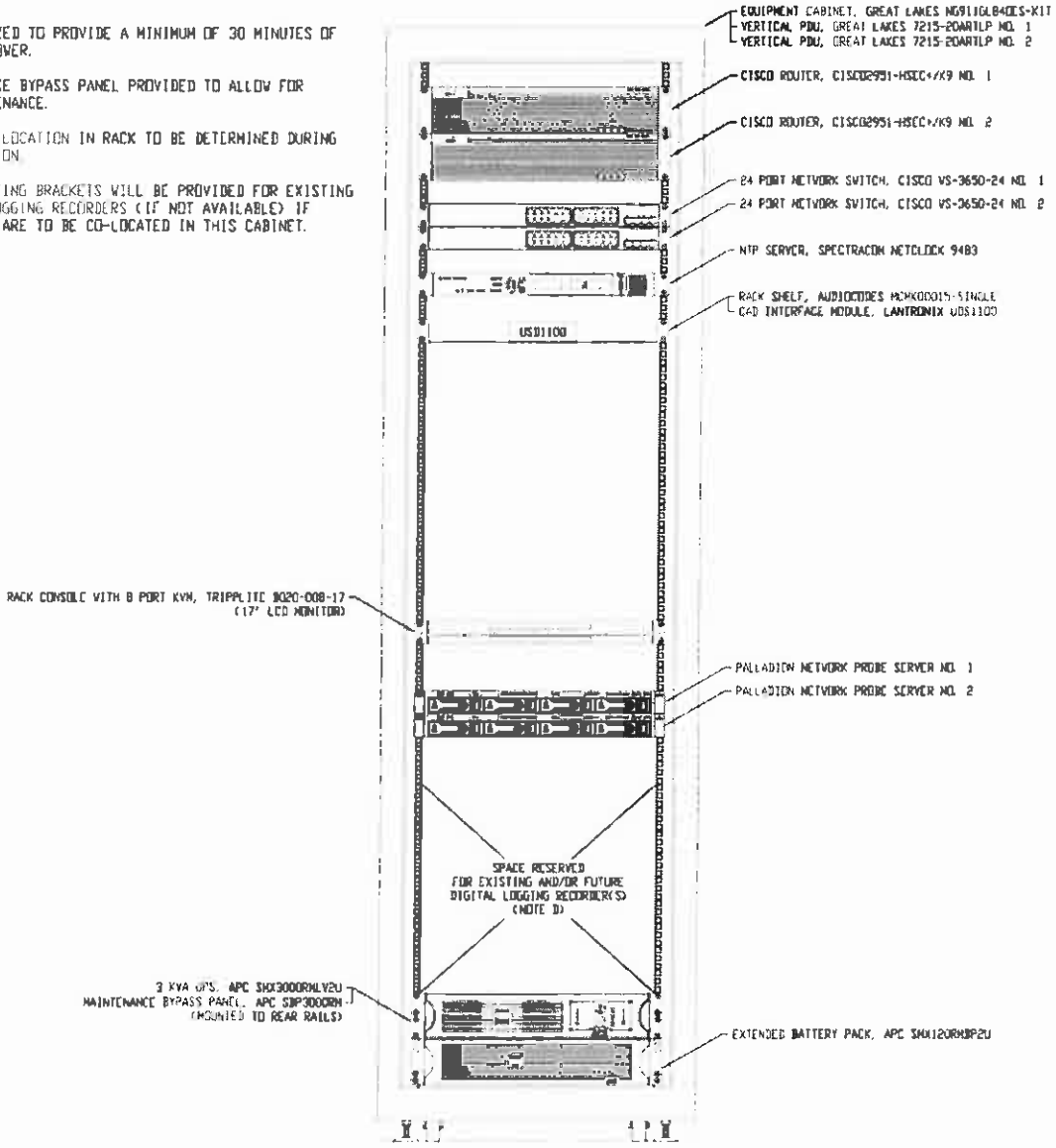
NOTES:

A UPS IS SIZED TO PROVIDE A MINIMUM OF 30 MINUTES OF BACK-UP POWER.

B MAINTENANCE BYPASS PANEL PROVIDED TO ALLOW FOR UPS MAINTENANCE.

C EQUIPMENT LOCATION IN RACK TO BE DETERMINED DURING INSTALLATION.

D RACK MOUNTING BRACKETS WILL BE PROVIDED FOR EXISTING DIGITAL LOGGING RECORDERS (IF NOT AVAILABLE) IF RECORDERS ARE TO BE CO-LOCATED IN THIS CABINET.



MEDIUM PSAP CABINET
ONE 30A CIRCUIT REQUIRED FOR EQUIPMENT CONNECTED TO UPS
(NINE (9) TO FOURTEEN (14) POSITION PSAPS)
(INCLUDES THREE (3) 10 POSITION TRAINING SITES)

MEDIUM PSAP (9 TO 14 POS) EQUIPMENT SCHEDULE				
RU	ITEM	QUANTITY	VOLTS	WATTS
2	CISCO2951-HSEC+/K9	2	110	60
1	24 PORT CISCO NETWORK SWITCH	2	110	150
1	NTP SPECTRACOM NETCLOCK 9483	1	110	40
0	LANTRONIX CAD INTERFACE MODULE	1	110	1.5
1	TRIPPLITE RACK CONSOLE	1	110	24
1	PALLADION NETWORK PROBE SERVER	2	110	400
2	APC 3KVA UPS (NOTE A)	1	110	50
2	APC EXTENDED BATTERY PACK (NOTE A)	1	110	N/A

ONE RU IS 1.75"IL

Figure 86. Preliminary Equipment Elevation – Medium PSAP (9–14 Positions)

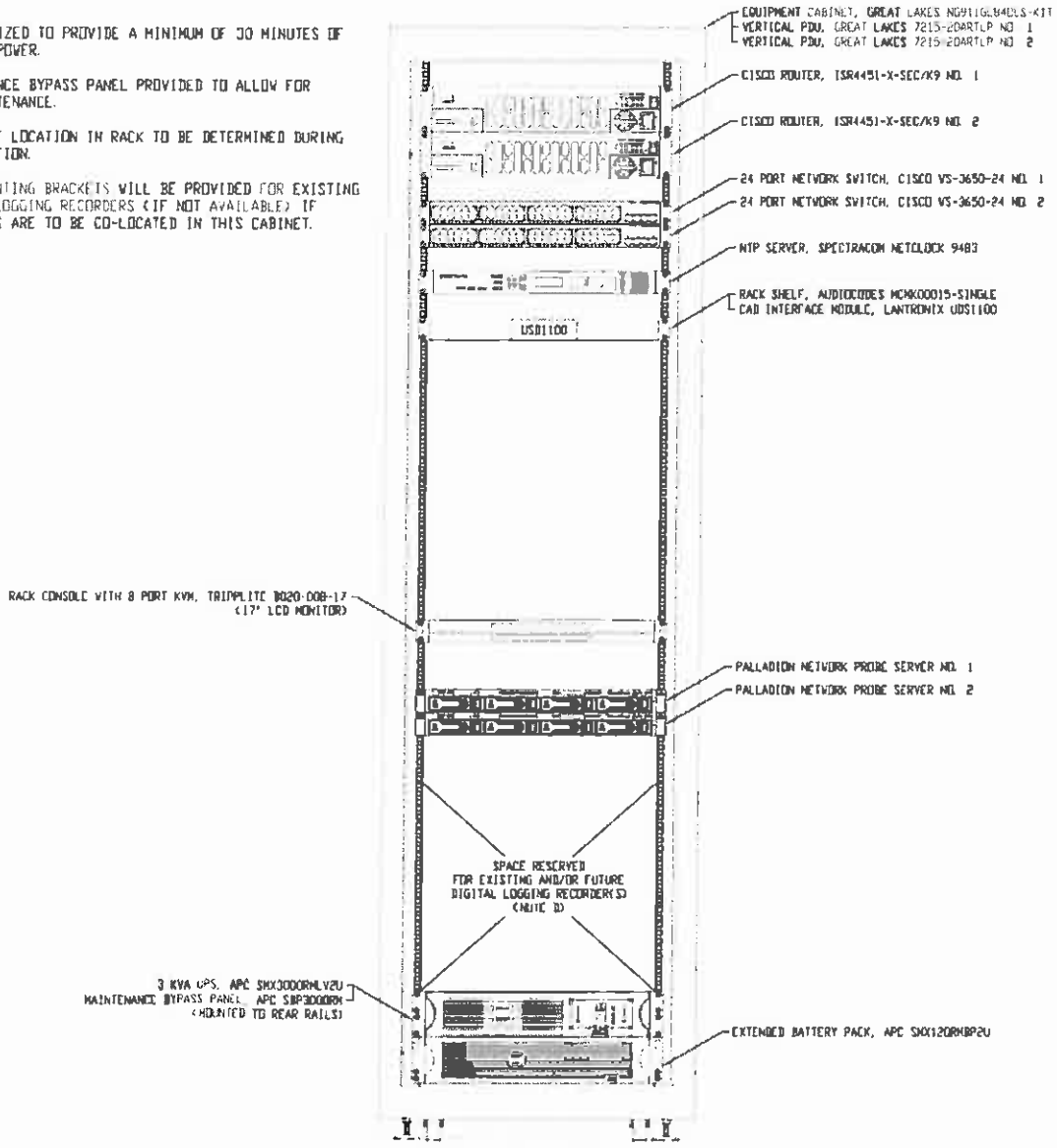
NOTES:

A. UPS IS SIZED TO PROVIDE A MINIMUM OF 30 MINUTES OF BACK-UP POWER.

B. MAINTENANCE BYPASS PANEL PROVIDED TO ALLOW FOR UPS MAINTENANCE.

C. EQUIPMENT LOCATION IN RACK TO BE DETERMINED DURING INSTALLATION.

D. RACK MOUNTING BRACKETS WILL BE PROVIDED FOR EXISTING DIGITAL LOGGING RECORDERS (IF NOT AVAILABLE) IF RECORDERS ARE TO BE CO-LOCATED IN THIS CABINET.



LARGE PSAP CABINET
ONE 30A CIRCUIT REQUIRED FOR EQUIPMENT CONNECTED TO UPS
(SEVENTEEN (17) TO FORTY-FIVE (45) POSITION PSAPS)
(INCLUDES ONE (1) 22 POSITION TRAINING SITE)

LARGE PSAP (17 TO 45 POS) EQUIPMENT SCHEDULE

RU	ITEM	QUANTITY	VOLTS	WATTS
2	ISR4451-X-SEC/K9	2	110	60
1	48 PORT CISCO NETWORK SWITCH	2	110	150
1	NTP SPECTRACOM NETCLOCK 9483	1	110	40
0	LANTRONIX CAD INTERFACE MODULE	1	110	1.5
1	TRIPPLITE RACK CONSOLE	1	110	24
1	PALLADION NETWORK PROBE SERVER	2	110	400
2	APC 3KVA UPS (NOTE A)	1	110	50
2	APC EXTENDED BATTERY PACK (NOTE A)	1	110	N/A

ONE RU IS 1.75"H

Figure 87. Preliminary Equipment Elevation – Large PSAP (17–45 Positions)

GDIT recommends two approaches to cabinet installation at the PSAP locations. The first involves mounting the cabinets to the concrete subfloor using threaded rods and appropriate fastening hardware. The second approach involves mounting the cabinets to the wall in the equipment room. Wall-mounted installation is only applicable for half-cabinets. Floor and wall space as well as site preference will determine which installation approach is employed. All back office equipment at the PSAPs will be rack-mounted within the equipment cabinet. GDIT will re-use the existing furniture and tables at the PSAPs for the new call taker equipment. Our proposed call taker equipment suite is shown in Table 31.

Table 31. Proposed Call Taker Equipment

Description	Vendor	Part Number	Dimension (HxWxD) inches	Remarks
911 Call Taker Workstation	Dell	OptiPlex 3020	11.4 x 3.6 x 12.3	
Workstation Monitor – 24" Fat Panel	Dell	P2414H	14.5 x 22.3 x 7.1	2 monitors per workstation
Workstation Sound Bar	Dell	AX510PA1	1.9 x 16 x 1.5	USB powered
Workstation UPS	APC	SMT1500RM2U	3.5 x 17.0 x 18.0 (63 lb.)	Floor-mounted beneath table
Workstation Maintenance Bypass	APC	SBP1500RM	3.5 x 17.0 x 3 (6.5 lb.)	Floor-mounted beneath table
Sound Point IP 650	Polycom	2200-12651-025	6 x 10.5 x 7.5	
35 Key programmable keypad	Fentek Industries	KPP35U	1.5 x 6.1 x 4.6	USB powered
IP Phone Headsets	Plantronics	CS540-XD	N/A	
Audio Interface Unit	Emergency CallWorks	EXC100001-NS		
Network Printer	HP	Laserjet Pro 400	10.7 x 14.4 x 14.5	

GDIT's site survey effort for each location will document details related to equipment delivery, storage, handling, and disposition. All aspects of our implementation will be planned and executed in a professional manager. GDIT will coordinate site access with the State 911 Department.

8.19.2.2. Grounding

All hardware and peripheral devices shall be mechanically and electrically grounded to prevent both user hazard and loss of data or hardware integrity due to external electrical impulse. The contractor shall demonstrate knowledge of local storm and lightning phenomena, and show such methods of protection in selection of local data transmission mode (i.e., shielded cable, fiber optics, etc.). The contractor shall ground all equipment installed by the contractor as specified in applicable standards.

The contractor shall ground all equipment in compliance with manufacturer recommendations and applicable standards. This shall include, but is not limited to, all servers, network equipment, appliances, metal conduit trays, cabinets, chassis, shelves, and transmission lines provided under this RFR.

The contractor shall furnish and install the required grounding and bonding conductors and make connections to the grounding system at the data centers, PSAPs and other sites.

GDIT will comply with the RFR specification.

GDIT draws on our global experience in understanding and implementing mission-critical communications solutions that fully accommodate and reflect local environmental conditions and associated codes and practices for ensuring performance and compliance, including for high lightning protection. GDIT's installation practices follow those of our equipment manufacturers

and draw on our over 40 years of experience working in the telecommunication industry, and more directly, in the public safety environment. GDIT will work with the manufacturer recommendations, applicable grounding standards, and UL-type best practices. GDIT will further include additional ground testing as part of our systems design and verification testing documents. After final ground testing, GDIT will include, as part of the as-built drawings, the location, and type of all grounding that was used.

8.20. WARRANTY, MAINTENANCE, AND MONITORING

System reliability and maintainability are major considerations driving the concept and design of the GDIT team's solution. GDIT recognizes the importance of system availability when public safety and life-saving responses depend on calls going through.

GDIT has provided mission-critical network operations support and sustainment services to the DoD, federal agencies, and state and local governments for over 20 years. We have established unparalleled expertise and capabilities in delivering support to our clients that range from full remote and on-site operational responsibility to advanced Tier III support. Our teammates expand the depth and scope of our support capabilities, providing additional experience and expertise in their respective products and core areas of support. GDIT and our subcontractors will provide a warranty for the system, including all hardware and software, for a period of one year from site acceptance. This will consist of a complete warranty covering all parts, labor, travel, and all other expenses.

Our performance under our current and prior contracts has enabled us to establish and maintain a highly qualified technical staff, comprehensive technical capabilities, and service delivery efficiencies with an established team of proven partners, and an extensive integrated logistics support network.

The overall architecture provided in this proposal is highly redundant to meet the Commonwealth's 99.999% availability requirements. The proposed system includes a state-of-the-art network management and reporting solution to monitor and operationally support the environment. GDIT will maintain and manage the entire network and all components as one complete system to ensure end-to-end service quality. A minimum of one-year warranty is provided for all elements included in our solution, if the OEM includes additional support that will be passed on to the Commonwealth.

Key Elements of the GDIT Team's Warranty, Maintenance, and Monitoring Operations

- Prevent problems from occurring through implementation of comprehensive maintenance program
- Mitigate problems by proactive monitoring to detect and correct problems before they occur
- Resolve issues using best practices at appropriate level
- Effectively staff operational and surge requirements drawing from a pool of employees, teammates, and partners located throughout the Commonwealth
- Provide a comprehensive turn-key solution for network operations and management

With the support of our NSOC, subcontractors, and OEMs, GDIT will ensure that during the warranty/maintenance period all of the systems installed will remain operational and free of defects. We will monitor facility and network operations to ensure continued performance to the specifications outlined in our engineering design.

8.20.1. Design and Operation

The contractor represents and warrants that the equipment, components, and services sold or provided in response to this RFR shall perform in accordance with their respective design specifications, and shall operate in accordance with the manufacturer's published specifications when operated and maintained in accordance with the manufacturer's recommendations for a minimum of one (1) year from their final acceptance by the State 911 Department.

GDIT will comply with the RFR specification.

GDIT warrants that the fully compliant solution provided to the Commonwealth, including all systems, equipment, components, software, and services, will operate and perform as designed, meeting all proposed specifications and all manufacturer specifications as published. This warranty period extends for one year from the date of final acceptance by the Commonwealth.

8.20.2. Configurations

The contractor represents and warrants that the configurations of equipment and services proposed in response to this RFR represent sound design principles and best practices being applied to provide a total system solution to the requirements stated in the RFR and referenced standards, and that the equipment and services provided shall operate together in a manner to perform the functions expressed in the RFR.

GDIT complies with the RFR specification.

The GDIT team is committed to delivering a fully compliant standards-based solution, utilizing both the proven best practices of the GDIT team and industry best practices. Most of the primary Original Equipment Manufacturers (OEMs) and partners in our proposal are recognized leaders in understanding and setting standards within NENA working groups and have invested significant time and effort at collaborative events, such as the NENA Industry Collaboration Event (ICE) meetings, and within the GDIT i3 Solutions Interoperability Lab.

Our solution is compliant with existing NENA i3 standards and reflects the outcome of examining multiple design alternatives and products in order to determine the best overall solution for the Commonwealth. Because the functional elements defined in the NENA i3 standards are integrated into the GDIT solution, the proposed systems are inherently designed for high levels of reliability and availability.

The architectural design of the proposed solution incorporates reliability and maintainability considerations while fully addressing the RFR requirements in all areas, including network management and operation, applications, appliances, statewide locations and facilities, and a solution that is interconnected in a robust and integrated IP environment. The configuration of proposed equipment and services will provide an interoperable and sustainable solution of systems meeting all of the Commonwealth's requirements specified in the RFR.

8.20.3. Equipment Models

The contractor represents and warrants that the equipment offered is standard new equipment, and the latest model of regular stock product, with parts regularly used for the type of equipment offered, and also that no attachment or part has been substituted or applied contrary to manufacturer's recommendations and standard practice. The

contractor shall furnish the current version of software or firmware for all systems provided. If a new version or release is issued after contract execution, but prior to the shipment of the system, then the State 911 Department shall have the option of substituting the new version or release in place of the originally proposed version or release, at no additional charge, after testing.

GDIT will comply with the RFR specification.

The GDIT team selected equipment based on performance considerations to best meet the requirements of the Commonwealth. GDIT warrants that all equipment to be furnished will be new, standard, and of current manufacture. Only the most recent models of equipment will be installed. All proposed equipment will be deployed in accordance the manufacturer's recommendations and standard practice.

The solution is designed for sustainability and longevity in both hardware and software, and it is intended to be operated and supported beyond the typical five-year product life cycle.

Current versions of software and firmware will be deployed with all systems provided. If new versions or releases are issued prior to a system being shipped, the Commonwealth may determine that the new version or release should be substituted, after testing. If the new version or release is used, there will be no additional charge to the Commonwealth.

8.20.4. Product Life Cycle

The contractor represents and warrants that the system components, including without limitation, the CPE, applications and appliances, data center equipment, are not currently at the end of their product life cycle. Bidders shall submit a statement identifying the length of time from site acceptance that contractor shall guarantee new (not reconditioned) parts availability. The contractor shall describe in detail the life expectancy of the system and system components. The life expectancy shall be a minimum of five (5) years from site acceptance.

Bidders shall detail the costs to upgrade the system components throughout the term of the contract for the total anticipated contract duration, including renewal options (ten (10) years). Bidders shall provide a detailed schedule of hardware refreshes.

GDIT will comply with the RFR specification.

The GDIT team's fully compliant solution is built from the ground up as a fully integrated NG9-1-1 system that has been designed using the latest and most advanced technology available today. This provides for long life expectancy, with equipment and systems fully supportable for five years and sustainable for at least ten years. GDIT guarantees new parts availability for a minimum of five years after site acceptance. This includes the CPE, applications and appliances, and data center equipment.

Costs to upgrade system components will be provided if requested by the Commonwealth, but the solution proposed can be utilized for the ten-year period of performance requiring only software upgrades and sustainment of the system as installed.

Costs for renewal options through ten years will be provided separately.

The GDIT team's CPE and call processing solution product roadmap and support timelines are not dictated by third-party manufacturers. The platform is intended to be 'evergreen' with a rolling upgrade cycle; there is not a point where the software will be end-of-life and replaced via fork-lift upgrade. All related hardware components are COTS and may be replaced with an alternate third-party product with limited effort.

The Java Enterprise web application which provides all 9-1-1 and CAD business logic and acts essentially as our ANI/ALI controller has been and continues to be developed by team member Emergency CallWorks directly, entirely within the United States. At the operating system and support utility level, the solution utilizes open source extensively. The primary benefit in utilizing open source software is the increased flexibility and control that having access to third-party source code provides. This provides us complete independence from all outside parties and much more independence than our competitors who do not have access to the source form of the numerous third-party software upon which they depend. With open source software we retain the option to 'self-maintain' the complete software stack in perpetuity. Also, we selected open source products which have a strong community and are typically supported by multiple vendors; something not possible with closed source software.

8.20.5. System Documentation

For each system, subsystem, and each type of equipment supplied, the contractor shall provide an electronic copy, and upon the request of the State 911 Department one complete printed set of maintenance manuals and/or technical documentation at the time of installation, with revised, final documentation provided within ten (10) business days after installation. Each piece of electrical equipment installed shall have a maintenance manual that depicts circuit diagrams, as well as proper unit assembly and installation. All drawings and maintenance manuals shall include all modifications and revisions made to the original drawings, and completely reflect the final layout and configuration of all installed hardware.

The contractor shall provide computer file copies of system layout and interface/interconnection point diagrams. Diagram files shall be provided in Visio file format and reflect the "as built" state of the system for the life of the contract. Any and all such documentation shall allow for the State 911 Department to copy information for import into the State 911 Department's records

This and all other system documentation shall be promptly delivered to the State 911 Department.

GDIT will comply with the RFR specification.

The GDIT team will provide electronic copies of the technical documentation needed to document and maintain the solution and configurations as required. When requested by the Commonwealth, paper copies will also be provided. Most hardware components are COTS and, therefore, include substantial assembly and installation documentation and maintenance manuals with circuit diagrams. GDIT will also provide design drawings at the time of installation and will "red-line" and update those documents to the final installed layout and configuration, to be submitted within ten (10) business days of installation completion.

System layout and interface/interconnection diagrams will be delivered in Visio file format and will reflect the as-built configuration of the system.

Other typical diagrams include: WAN topologies, LAN topologies, cabinet and rack elevations, and points of demarcation.

All documentation will be delivered promptly to the State 911 Department.

8.20.6. Maintenance and Monitoring

The GDIT team will provide an integrated, Commonwealth-based maintenance and monitoring solution that complies fully with the RFR.

8.20.6.1. Warranty Period

The contractor represents and warrants that the system, including all hardware and software, shall operate in conformance with the specifications for the system and shall be free from defects in materials and workmanship, for a period of one (1) year from site acceptance. This shall consist of a complete warranty covering all parts, labor, travel and all other expenses. The contractor represents and warrants that the contractor shall modify, adjust, repair, and/or replace said system as the State 911 Department deems it to be necessary or appropriate to have the system perform in full accordance with the terms and conditions of the contract. Warranty repairs on all furnished equipment, systems and software shall be made at no cost for a period of one (1) year from the date of site acceptance.

Bidders shall describe how system and equipment maintenance and repair will be handled during the warranty period. During the warranty period, the contractor shall respond to all repair calls or notices of system malfunction at no additional cost to the State 911 Department.

The contractor shall have qualified technicians that shall commence repair to catastrophic system malfunction within one (1) hour, major system malfunction within two (2) hours, high priority system malfunction within eight (8) hours, and standard priority system malfunction within two (2) business days during the warranty period.

The State 911 Department reserves the right to determine, in its sole discretion, whether a system malfunction is classified as catastrophic, major, high priority, or standard priority.

The contractor shall be responsible for any shipping costs incurred to send components to manufacturers for repair or replacement. The State 911 Department reserves the right to closely monitor and observe warranty repair service.

During the warranty period, the contractor shall maintain adequate staff and spare parts inventory, both located within the Commonwealth, to ensure prompt warranty service.

Any subcontractor costs for the first-year warranty of any system hardware or software component covered under the above warranty requirements shall be included within the base system proposal price. The State 911 Department shall pay no maintenance costs during the warranty period.

GDIT will comply with the RFR specification.

All equipment, software, and services furnished by GDIT will be warranted free of defects in material and workmanship, will operate within the proposed and manufacturers' specifications, and will include the following elements of warranty support for at least one year following acceptance:

- Alarm monitoring and response
- 24x7 support via our help desk and NSOC in the Commonwealth
- On-site service response by qualified technicians
- Maintenance of spare parts inventory (see Section 8.20.18, Spare Equipment Repair and Replacement), and replacement of defective hardware
- Remote technical assistance from the GDIT team and OEM technical assistance resources
- Software patching
- Travel cost for warranty issues
- All shipping charges associated with the transport and return of defective components

GDIT will perform all necessary warranty repairs, adjustments, or modifications will be performed at no cost to the Commonwealth for a period of one year from the date of site acceptance, responding to all repair calls or notices of system malfunction.

The GDIT team will perform all necessary maintenance, including modifications, adjustments, repairs, and/or replacements of hardware and software as the State 911 Department deems it to be necessary or appropriate to have the system perform in full accordance with the terms and conditions of the contract.

All maintenance, monitoring, and repair activities will be coordinated through the GDIT Help Desk and NSOC in Needham, MA using Commonwealth-tailored versions of our proven tools, processes, and procedures, ensuring that the Commonwealth's systems operate at peak performance.

Proactive monitoring of the network, data centers, and other systems and facilities is performed as a key component of our overall maintenance concept. The GDIT NSOC receives key data and performance indicators self-generated by the systems and live traffic within the solution. This data and information is incorporated in our network management system for analysis and reporting and identification of potential issues.

Proactive maintenance also includes continual updates of software to ensure the integrity of operational systems. This maintenance is scheduled and performed in collaboration with and with the approval of the Commonwealth, with consideration given to the risk, impact, and reasons for such maintenance, and with recommendations for applying the maintenance patches and upgrades in a manner that best meets the requirements. Typically, such maintenance is performed remotely, leveraging the redundant nature of the systems to ensure no impact to services. Where on-site maintenance is warranted, the GDIT team will provide the necessary technicians.

The GDIT team has trained and qualified technicians in the Commonwealth that will commence on-site repair activities for system malfunctions within the time frames specified for catastrophic, major, high-priority, or standard-priority malfunctions.

- Repair of catastrophic malfunctions will commence within one hour
- Repair of major malfunctions will commence within two hours.
- Repair of high-priority malfunctions will commence within eight hours.
- Repair of standard-priority malfunctions will commence within two business days.
- Remote repair activities from our Help Desk and NSOC will commence immediately for catastrophic, major, and high-priority malfunctions.

During the warranty period, GDIT will ensure that sufficient technical staff and spare parts inventory are retained within the Commonwealth to ensure warranty service that meets these time frames.

All subcontractor costs for the first-year warranty of system hardware and software components covered under the warranty requirements is included within the base system proposal price. The State 911 Department will not be billed for any maintenance costs during the warranty period.

8.20.6.2. Maintenance Following End of Warranty Period

After the one (1) year warranty has expired, the contractor shall provide maintenance services on a 24 x 7 basis under the same terms and conditions as during the warranty period as described above. Maintenance shall include all parts and labor, monitoring the system for alarm conditions and responding to such alarms, and all other expenses necessary to support the system.

The contractor shall have qualified technicians that shall commence repair to catastrophic system malfunction within one (1) hour, major system malfunction within two (2) hours, high priority system malfunction within eight (8) hours, and standard priority system malfunction within two (2) business days.

The State 911 Department reserves the right to determine, in its sole discretion, whether a system malfunction is classified as catastrophic, major, high priority, or standard priority.

GDIT will comply with the RFR specification.

The same maintenance services provided during the warranty period will continue following expiration of the one-year warranty period. The same terms and conditions as described in Section 8.20.6.1 (Warranty Period) will apply to the post-warranty maintenance period, including the response times.

The transition from warranty to post-warranty support will be seamless and transparent. The same facilities, personnel, and processes will remain in place, providing the same level of support for the Commonwealth.

8.20.6.3. Equipment Replacement

During and after the warranty period, any equipment that must be replaced as a result of conditions covered under warranty shall be replaced with new equipment of the equivalent or better make and model.

GDIT will comply with the RFR specification.

The GDIT team will stage spare parts and equipment at multiple locations in the Commonwealth to ensure rapid deployment when replacements are required for malfunctions. The replacement equipment will be new equipment, not used or refurbished, and it will be the same, or better, make and model as the equipment being replaced.

8.20.7. Customer Support Services

During and after the warranty period, the contractor shall monitor all components of the system 24 x 7 to immediately identify potential problems or outages and shall make necessary notifications, consistent with notification procedures established by the State 911 Department. The contractor shall isolate and repair all identified problems. The contractor shall provide an escalation plan and procedures to ensure service response times that meet or exceed the standards set forth in 560 CMR 2.00, as may be amended from time to time.

Within sixty (60) days of contract award, the contractor shall develop and submit to the State 911 Department for approval an operations manual that outlines NOC and help desk operational procedures for supporting the Next Generation 911 system.

The contractor shall provide the following customer support services for all services provided under the contract and any renewals thereof:

GDIT will comply with the RFR specification.

The GDIT team is able to provide a full array of customer support services covering all areas of ongoing program operations and maintenance support. GDIT is ready to provide all ongoing warranty, monitoring, and O&M services support to the MA NG9-1-1 project. This includes personnel and facilities that can fulfill any of the activities associated with the required functions as outlined in the RFR and our proposal. O&M service will be managed from our Needham, MA facility which is a 24x7x365, combined NSOC and program-specific help desk. This will provide "one-stop" user support for customer queries, issue tracking, escalation, initial configuration, troubleshooting, repair, network operations, monitoring, and maintenance. Services provided include:

Figure 88. GDIT's Massachusetts-Based Support Services

- Technician Dispatch Support
- Systems Monitoring
- O&M Repair and Maintenance Services
- O&M Purchasing Support
- Warranty Support
- Inventory Management
- Preventive Maintenance
- Deployment Equipment Support
- Logistics/Warehouse Support
- End User Training
- Labor Services and Support

Our team's customer support will include responding to reported troubles, proactively maintaining the installed equipment and systems, and actively monitoring all components remotely at the NSOC. When potential problems or outages are identified, the Commonwealth will be notified according the procedures established by the Commonwealth and troubleshoot and resolve the issues.

The GDIT team will develop and provide an escalation plan and procedures outlining how the different types of malfunction classifications (catastrophic, major, etc.) will be addressed to ensure that the required notifications are provided and the required response times set forth in 560 CMR 2.00 are exceeded or achieved.

Within the first 60 days of the contract, GDIT will develop an operations manual and submit it to the Commonwealth. This operations manual will be based on our existing and proven NOC, SOC, and help desk procedures, tailored for the unique conditions and requirements of the Commonwealth's NG9-1-1 system.

8.20.7.1. Help Desk

Throughout the term of the contract and all renewals thereof, the contractor shall operate a help desk for the purpose of receiving, logging, tracking, dispatching, and reporting on trouble calls. The help desk shall be fully operational and staffed on a 24 x 7 basis. There shall be supervisory staff on-site at the help desk on a 24 x 7 basis.

The help desk shall be located in the United States, with a strong preference that the customer service center be located within the Commonwealth. The help desk shall be adequately staffed so that calls to the help desk are

answered by live help desk staff that are trained and qualified on the systems and services furnished under this RFR. Calls shall not be answered by an automated attendant or other automated means.

The help desk shall serve as a single point of contact for PSAPs for all matters, including without limitation, the system and all components of the system. The help desk shall have the ability to communicate directly and immediately with maintenance and support services for the system and all components of the system, including without limitation, network troubles.

The help desk shall have the authority to dispatch maintenance staff from all contractors, manufacturers, subcontractors and other entities responsible for any components or services contracted for through this RFR. The contractor shall dispatch staff in a timely manner to meet the response time requirements stated in the RFR.

The contractor shall provide a dedicated toll-free 24 x 7 service number to respond to troubles relating to the system or any components of the system. When reported 911 system troubles or failures are received, the contractor shall open a trouble ticket and shall prioritize and isolate the trouble. The help desk shall direct, prioritize, escalate, and oversee the repair of any and all reported 911 system failures and/or trouble tickets.

The contractor shall provide specially trained technicians to proactively identify problem areas impacting the quality of service and to serve as the liaison between the PSAPs and the contractor. The help desk shall open a ticket for all calls received. Any and all troubles that do not fall under the direct responsibility of the contractor shall be forwarded to the appropriate party.

The contractor shall provide the State 911 Department with read-only access to the help desk system to run reports. The contractor shall grant the State 911 Department read-only real-time access the contractor's trouble ticket reporting system.

Bidders are advised that the State 911 Department reserves the right to conduct a site visit of the facility from which the bidder proposes to provide help desk support. Further, the State 911 Department reserves the right to conduct a site visit of the facility from which the contractor provides help desk support at any time during the term of the contract.

GDIT will comply with the RFR specification.

GDIT will locate the help desk in Needham, MA specifically for the MA NG9-1-1 project, which will be the focal point for all communications from the PSAPs. The help desk will also be our team's central point of contact for all warranty, maintenance, and support service operations, coordinating and facilitating communication among GDIT's partners, subcontractors, vendors, OEMs, and other internal and external entities involved in maintenance operations.

The GDIT help desk will be collocated in the same facility with the NSOC, and the Commonwealth will benefit from the reduced reaction time and improved communication between the help desk and NSOC personnel this affords, as they coordinate team response to maintenance actions. The facility also houses our extensive i3 Solutions Interoperability Lab environment, utilized for testing and proving patches and upgrades prior to rollout to eliminate any related maintenance issues. The help desk will serve more broadly as the Commonwealth-located customer service center, as the center of program operations, and as the liaison between the PSAPs, technical staff, partners and vendors, and other support personnel involved in the project.

The help desk will open tickets for all calls received using our existing Remedy ticketing system and provide the first tier of technical support by prioritizing, troubleshooting, and isolating problems. The help desk will authorize and coordinate the dispatch of maintenance personnel, when required, and will escalate issues to the appropriate teammates and OEMs.

Figure 89 illustrates the standard flow of a trouble ticket, from receipt of the initial call through ticket closeout.

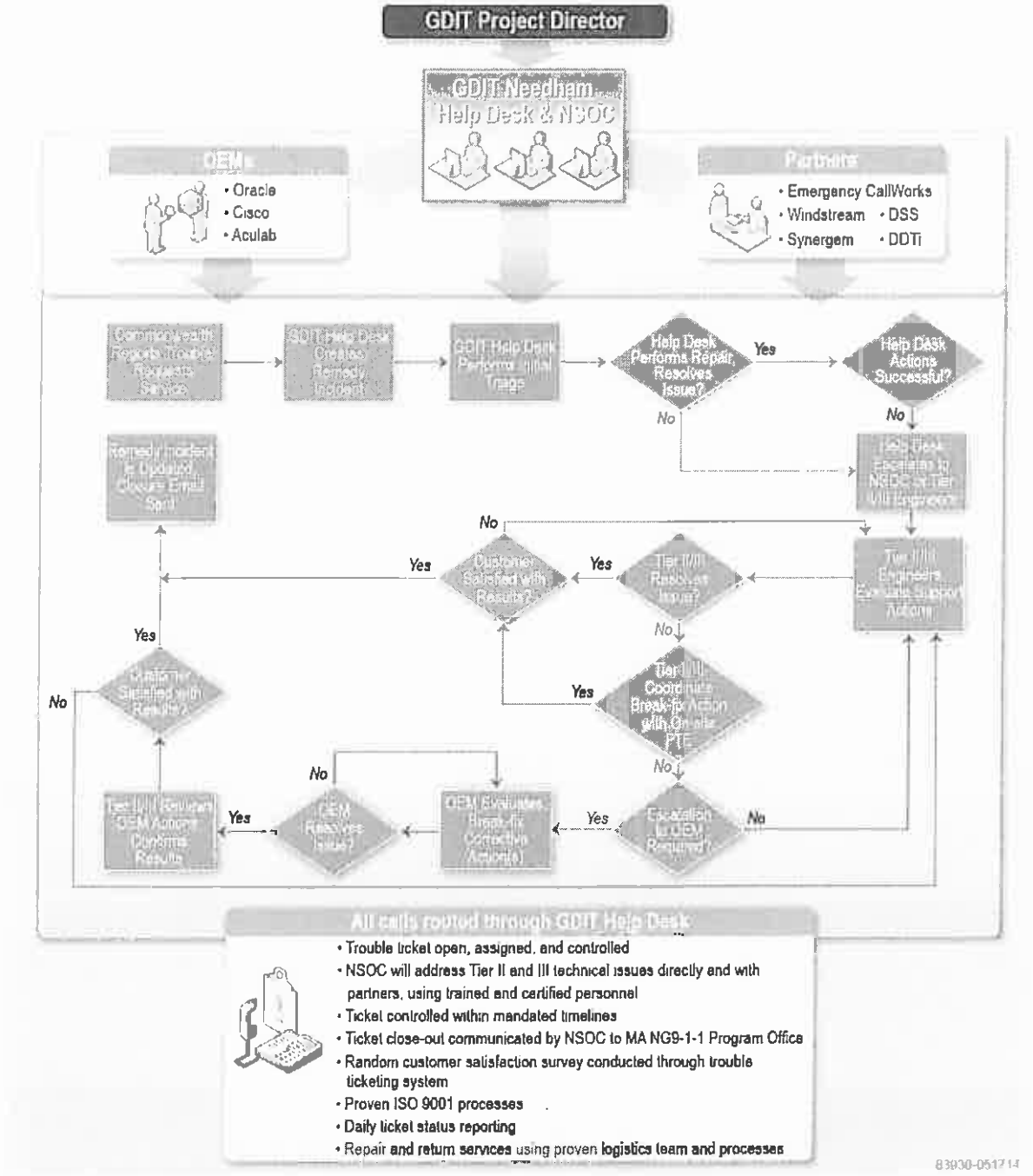


Figure 89. Trouble Ticket Flow

Help desk personnel will proactively work each issue and manage tickets to completion, actively coordinating with all stakeholders and subject matter experts, keeping all lines of communication open, and driving all parties to collaborate and resolve issues, while thoroughly documenting progress and resolution for each ticket. The help desk will be operational 24x7x365, with supervisory staff always on duty, and will be reached via a dedicated toll-free service number.

The GDIT Needham help desk and NSOC data center backup diesel generator provides 24-hour continuous power. The data center also has internal Uninterrupted Power Supply (UPS) systems providing 30 minutes of automatic backup battery. A one-hour service agreement is in place for fuel replenishment should there be an extended use of the backup generator. In the event of a natural disaster or other severe event that limits use of the facility, our help desk and NOC in Fairview Heights, IL will take over, utilizing the same Remedy ticketing system. That facility is staffed 24x7, is served by a 50 KVA natural gas backup generator, and has the same call-processing capabilities as the Needham help desk.

GDIT will provide the Commonwealth with read-only access to our Remedy ticketing system for the purpose of running reports and for real-time ticket status. This open access has proven to be very effective for customers in our current implementation and maintenance contract with the Federal Aviation Administration (FAA). Customer personnel regularly use their access to the ticketing system to gain real-time status updates and information rather than using time-consuming phone calls and emails to request updates.

8.20.7.1.1. Help Desk Software Tools

The help desk shall be equipped with appropriate software tools to initiate trouble tickets, and shall track and monitor the progress of trouble tickets.

The software tools shall be configured to allow authorized users from the State 911 Department or individual PSAPs to initiate trouble tickets electronically, to track and monitor the status of trouble tickets, and to view and create management reports.

The help desk and the NOC shall have the ability to access the contractor's trouble ticket reporting system for all aspects of the system, including without limitation, the applications and appliances at the data centers and CPE, and shall communicate directly with each other regarding troubles.

The GDIT help desk utilizes a customizable Remedy trouble ticketing system. This will be configured to allow the NSOC, the Commonwealth, and other stakeholders to initiate, track, and monitor tickets, and to also create and run management reports. All tickets will be tracked and managed using the centralized Remedy system.

An example screenshot of our Remedy ticketing system is shown as Figure 90.

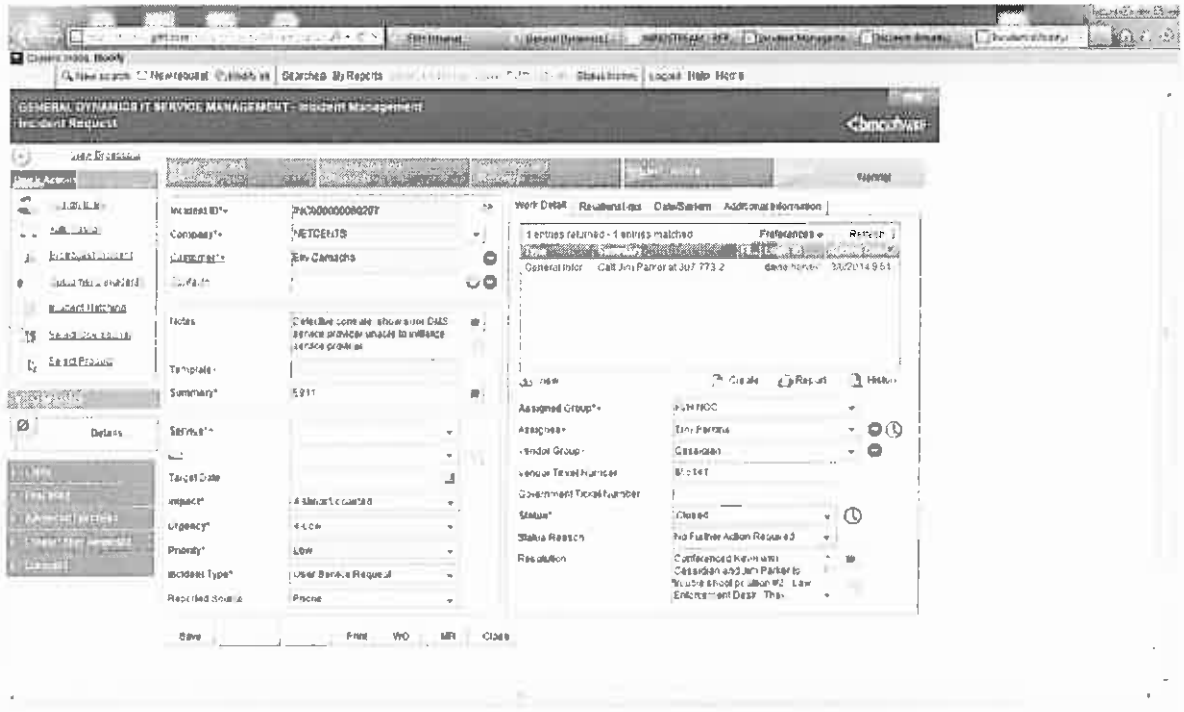


Figure 90. Remedy Ticketing System Screenshot

8.20.7.2. Repair of Troubles

The contractor shall maintain dedicated technicians who are fully competent, trained, qualified, and knowledgeable with respect to the network, applications and appliances, and CPE of the system and all components of the system.

The contractor shall undertake commencement repair, as defined in Section I- Definitions, within four (4) hours of any application, appliance, or CPE failure, and shall undertake commencement of repair, as defined in Section I-definitions, within two (2) hours when call processing is affected or when otherwise required.

The contractor shall provide on-site service response by field technicians who are fully competent, trained, qualified, and knowledgeable with respect to the applications and appliances, and CPE as described herein, within four (4) hours of trouble identification when call processing is affected or when otherwise required.

The contractor shall provide the necessary number of dedicated on-site regional supervisory service technicians located within the Commonwealth within fifty (50) miles of each PSAP, who are fully competent, trained, qualified, and knowledgeable with respect to the network, database, and CPE as described herein and are responsible for ensuring satisfactory resolution of all emergent and non-emergent service-related issues on a regional basis with allowance of "on-call" coverage by supervisory service technicians from other regions to ensure uninterrupted, 24 x 7 coverage by such supervisory personnel. The geographic regions, to be mutually agreed upon by the State 911 Department and the contractor, assigned to such regional supervisory service technicians shall ensure appropriate statewide service coverage. The regional supervisory service technicians shall act as the single point of contact with the service center technicians and the State 911 Department for the region.

GDIT will comply with the RFR specification.

Our service team, located in the Commonwealth, is staffed with highly trained and knowledgeable personnel on a 24x7x365 basis and will respond to troubles relating to components or systems necessary to complete 9-1-1 calls through to the PSAP or for call handling purposes. When reported system troubles or failures are received, or when our monitoring systems and proactive network management processes identify an issue, our help desk personnel immediately begin the repair process of clarifying the report and prioritizing the

trouble. When remote troubleshooting by the NSOC or our team's subject matter experts will not remedy the issue, we will dispatch on-site service technicians within the following time frames:

- Within four hours of any application, appliance, or CPE failure
- Within two hours when call processing is affected, or as requested by the Commonwealth

Our team has trained and qualified supervisory field technicians located within 50 miles of each PSAP and additional field technicians strategically based at locations around the Commonwealth for optimal coverage. The regional supervisory technicians will also be available to support incidents, to be on call, and to perform dispatches themselves. This ensures overlapping 24x7 capability for dispatches to all system locations. With our own technicians and multiple subcontractor partners, response times will be assured even in the event of illness, vacations, or other availability issues.

GDIT will employ a tiered support approach, where technicians are supported by remote and (as required) on-site subject matter experts to ensure the proper resources are always available. The on-site resources and interactions will be tracked and managed by the GDIT help desk using an action register and managing planned resolution activities. All technicians will undergo continuous training by GDIT and our product partners to ensure their knowledge and skills are fully maintained and up-to-date over the period of performance.

Upon award, we will work with the State 911 Department to determine the most efficient geographic regions to fall within the responsibility of a single supervisory service technician. The supervisory technicians will support each other for surge capability and for on-call and backup coverage in the event of severe weather, traffic problems, or other disruptions to travel.

These regional supervisors will be the single point of contact for their service area technicians and for the State 911 Department in that region.

8.20.7.3. Network Security and Operations Center

The contractor shall provide monitoring, maintenance and support services throughout the term of the contract and all renewals thereof. The contractor shall operate a network operations center, or NOC, on a 24 x 7 basis. The NOC shall provide constant monitoring and dedicated network management services and shall interface with the contractor's help desk, the contractor's technicians, and various carriers providing network connectivity to diagnose and repair network outages. There shall be physical diversity and diverse aggregation points for network monitoring from the NOC to the aggregation points. The contractor shall continually monitor the system for performance issues, faults and failures, utilizing a staffed network operations center with properly trained and certified live personnel providing diagnostic, re-route, trouble ticket issuance, service dispatch and help desk functionality on a 24 x 7 basis. Bidders shall describe in detail the NOC proposed, including without limitation, details about the location, staff, training, standard operating procedures, provisions for disaster recovery and redundancy, and location, equipment, and software currently in use. The contractor shall utilize simple network management protocol for the management and monitoring of the system and shall utilize encryption, verification or message integrity and authentication to provide security for the system. The NOC shall be located in the United States.

The contractor may be required to train Commonwealth personnel on the function of the NOC and the network monitoring software for eventual transition to takeover by Commonwealth personnel. Costs relating to such training will be negotiated at the time the Commonwealth elects to engage the contractor for the provision of these services.

The NOC shall be designed and configured to monitor the entire network, including but not limited to, connections between the data centers and PSAPs, connections within the data centers and PSAPs, and external connections from communication service providers and the Internet.

The NOC shall be staffed by individuals trained and experienced in telecommunications networking and the Next Generation 911 system on a 24 x 7 basis. The NOC staff shall have immediate access to the contractor's engineering resources for trouble escalation and resolution. The engineering resources shall have advanced knowledge of all system components, configurations, and applications, and shall have internetworking, network security, and other skill sets necessary to troubleshoot and repair complex problems throughout the system. The NOC shall maintain a dedicated toll-free 24 x 7 service number for the purpose of accepting calls from the State 911 Department, EOPSS/OTIS, help desk, carriers, and other parties relating to the system or any components of the system. The NOC shall perform trouble shooting and diagnose network performance problems. The NOC shall automatically generate trouble tickets for outages.

The NOC shall be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure.

- *The NMS shall continuously monitor the performance and availability of all devices, network connections, applications, CPE, and other functional elements throughout the Next Generation 911 system on the network;*
- *The NMS shall monitor network performance, including throughput, latency, jitter, packet loss, MOS and other parameters, including any performance criteria set forth in this RFR;*
- *The NMS shall monitor the network for network intrusion attempts, security breaches, issue network security alerts to the network services provider and State 911 Department staff, maintain logs of all activities that may indicate potential security breaches, and initiate appropriate predetermined responses to potential security breaches (such as blocking traffic or disabling an account);*
- *The NMS shall create alarms based on thresholds and parameters developed in concert with the State 911 Department, distribute alarm notifications to appropriate contractor and State 911 Department staff by telephone, email, texting or other means, initiate remedial processes;*
- *The NMS shall monitor the environment at all data centers where critical network components are housed, including temperature, humidity, equipment room physical security, etc. If not already in place and operational at the time of contract award, the contractor shall furnish and install necessary sensors and connectivity to support this requirement;*
- *The NMS shall monitor ancillary network components such as power utilization and backup power systems (including generator status, fuel levels, battery condition, etc.);*
- *All NMS services supporting the network shall be available to the State 911 Department and OTIS over a secure web-based interface. The NMS shall allow up to five (5) simultaneous users with no degradation to the network operations or performance. The NMS shall allow multiple levels of access based on logon and password;*
- *In the event of any service-affecting outage, the NOC shall, within fifteen (15) minutes of the onset of the outage, notify through a single point of contact a designated State 911 Department and PSAP representative(s) and other personnel as identified by the State 911 Department via telephone or other electronic means (e.g., Email, text, etc.). Additional notifications shall be sent at least once every two (2) hours while the outage continues.;*
- *In the event of a non-service-affecting outage (i.e., failure of a major network component that may not directly affect service due to network redundancy, but which reduces the level of available redundancy), the NOC shall notify through a single point of contact a designated State 911 Department, and PSAP representative, and other personnel as identified by the State 911 Department via telephone or other electronic means (e.g., Email, text, etc.) within one (1) hour during normal business hours or if after hours at the beginning of the next business day;*
- *In addition to real-time performance monitoring, the NMS shall prepare historical reports quantifying the performance of the networks (at no additional charge to the State 911 Department). Standard reports shall include call counts by type, origination point, destination PSAP, latency, jitter, packet loss, throughput, traffic volumes, up time, alarms received, and a description of responses and resolutions. All incidents shall be time stamped. Reports shall be able to be prepared on an hourly, daily, weekly, monthly, and annual basis. Trend analysis shall also be included in these historical reports. Reports shall be provided in electronic format using commonly available office software to facilitate sorting and analysis of data; and*
- *The network performance monitoring tools shall be industry standard platforms designed for and deployed by network operators on networks of the same size and complexity as the Next Generation 911 network.*

Bidders are advised that the State 911 Department reserves the right to conduct a site visit of the facility from which the bidder proposes to operate its NOC. Further, the State 911 Department reserves the right to conduct a site visit of the facility from which the contractor operates its NOC at any time during the term of the contract.

GDIT will comply with the RFR specification.

The GDIT NSOC will provide 24x7 coverage and a direct path for escalation and remediation, for managing OEM and teammate support, for providing dispatch of additional subject matter experts, and for managing maintenance activities and spares inventories. GDIT's expectation and experience is that our NSOC's services will help the Commonwealth maximize the efficient use of staff, reduce systems maintenance activities, and ensure the availability of all systems.

Our NSOC personnel hold OEM and industry certifications for a wide array of OEM products and technologies, and we maintain direct relationships with OEMs and their support and technical staff, which enables us to gain a level of support, visibility, and awareness that is unique, even among large system integrators.

GDIT's maintenance and repair approach utilizes our 24x7x365 NSOC located in Needham, MA, with a backup 24x7x365 Network Operations Center (NOC) located in Fairview Heights, IL and a backup Security Operations Center (SOC) in Herndon, VA. Our NSOC is staffed and run by GDIT personnel. These facilities provide centralized, multi-tiered support to a host of programs and customers, and possess personnel and equipment to remotely support legacy and IP communication systems, including E9-1-1 and NG9-1-1 systems. The NSOC will work closely with the Help Desk, the network providers, Emergency CallWorks, dispatch technicians, and other teammates and vendors to ensure that the Commonwealth has one seamless interface for coordination of all maintenance and repair issues.

The Needham NSOC is collocated in the same facility as the help desk, GDIT's Unified Communications (UC) engineering team, the technical labs, and the project office headquarters. This will ensure efficient communication among the team, rapid troubleshooting, and proof of concept testing. This location also allows for significant surge staffing capability, with the deep pool of UC engineering resources available to work with, and supplement, the NSOC team on any specific issue. The NSOC engineering staff, with significant on-call coverage and capabilities, is also able to dispatch, as needed, to assist technicians on site with problem solving and analysis. The team's engineering resources have advanced knowledge of all proposed system components, configurations, and applications. Additional expertise in networking, network security, telecommunications, unified communications, information technology, and other disciplines are represented in the in-place team. This will enable the team to troubleshoot and resolve complex issues and problems throughout the proposed system.

The NSOC will utilize physical diversity and diverse aggregation points for network monitoring from the NSOC to the aggregation points.

GDIT will maintain a dedicated toll-free service number to be used by all stakeholders in reporting and coordinating maintenance reporting and activities. Trouble tickets and notifications will be automatically generated in the event of an outage. Our LEC partner, Windstream, will monitor the network end-to-end to the edge routers at the PSAPs and data centers. GDIT and Windstream will integrate the flow of alarms and information from their network monitoring systems, with all maintenance communication and coordination flowing through the GDIT help desk and NSOC.

Windstream utilizes a suite of monitoring tools and methods to provide proactive notification of server- or service-affecting events. These methods include automated messaging sent from management/monitoring systems that automatically notify personnel that a service is down or impaired.

The GDIT team utilizes a Network Management System (NMS) that consolidates a suite of monitoring tools and methods to provide proactive notification of server or service-affecting events. These methods include automated messaging sent from management and monitoring systems that notify personnel directly without any intervention that a service is down or impaired.

Proactive monitoring for changes in the environment outside of normal operating conditions prevents incidents from occurring that may lead to a service outage or impairment for a user organization. A conceptual diagram of the NMS is shown in Figure 91.

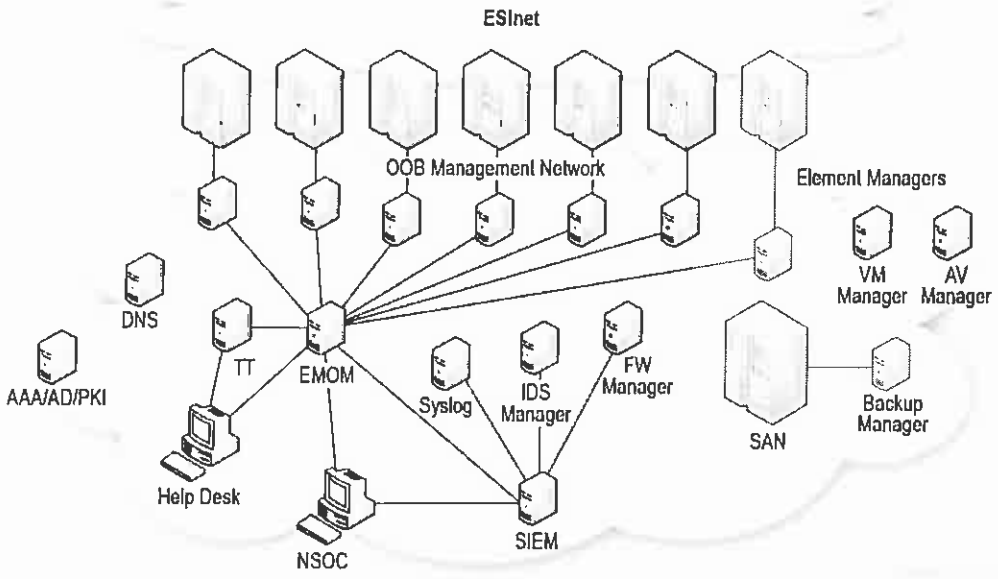


Figure 91. GDIT's Massachusetts NG9-1-1 Network Management System

Options for monitoring systems include SNMP-based metrics for system health (CPU utilization, drive space, memory usage), service or daemon status (service up/down), or standard TCP/IP protocol response (ping, http, https, smtp, ftp), as well as non-standard application-dependent port response.

GDIT's proposed NMS solution includes:

- **Oracle Palladion** – Each BCF has packet inspection capabilities that allow for measurement of media and reporting of service path signaling. This information allows for the direct assessment of service quality and for proactive maintenance, and provides critical information for reactive diagnostics and maintenance.

- **SolarWinds Server and Applications Monitor (SAM)** – SAM provides application and server monitoring, alerting, reporting, and server management, including monitoring for server operating systems, network interfaces, services, process, and applications. SAM also monitors the hardware-specific health and performance components such as CPU, hard drive, power supply, fan, memory module, and array status.

- **SolarWinds Network Performance Monitor (NPM)** – NPM provides network fault and availability management for proactive detection, diagnosis, and resolution of network issues, and tracks response time, availability, and uptime of multi-vendor routers, switches, and other devices. NPM shows performance statistics in real-time via dynamic network maps, and has a customizable dashboard to provide insight into the network's health.

- **SolarWinds Network Configuration Manager (NCM)** – NCM performs configuration management actions for NPM alerts and takes a detailed inventory of network devices, and builds and maintains a configuration management database. NCM can track Internetwork Operating System (IOS) software and versions and enables IOS/firmware updates using a Trivial File Transfer Protocol (TFTP) server or via FTP, HTTP, or other protocol.

- **SolarWinds netFlow Traffic Analyzer (NTA)** – NTA captures and converts continuous traffic data to provide charts and tables on network usage. It creates detailed network traffic reports based on applications, protocols, endpoints, and resources. It also provides bandwidth alert notifications for exceeding defined thresholds.

- **SolarWinds Database Performance Analyzer** – Database Performance Analyzer focuses on instance response time, finding the root causes of delays inside of database servers. It tracks every query in every session, and captures the server wait types that impose delays on the query. Database Performance Analyzer correlates other essential statistics to give a complete understanding of performance problems.

Using the NMS, NSOC personnel will monitor the performance and availability of all devices, network connections, applications, CPE, and other functional elements of the system and network 24x7x365. The NMS will generate alarms for conditions and parameters that meet predetermined thresholds established in concert with the State 911 Department. The NMS will automatically distribute notifications, via email and text messaging, to the GDIT NSOC and engineering team as well as members of the State 911 Department staff. Our Remedy ticketing system provides immediate email and text notifications to the NSOC Manager and key engineering and upper management personnel when a critical ticket is opened. All available GDIT team resources will be devoted to quickly responding to, and resolving, critical outages.

The State 911 Department and the Office of Technology and Information Services (OTIS) will be given access to the NMS tools and reports via a secure, web-based interface that will support five simultaneous users. Commonwealth staff will also be trained on the NSOC systems, procedures, and NMS to facilitate possible future takeover of the operations by Commonwealth personnel.

Sensor-based environmental and power system monitoring will be performed at each of the data centers with automatic notification to the NSOC of any conditions that exceed defined thresholds.

In the event of a non-service-affecting outage (only redundant capabilities affected), the NSOC will notify appropriate Commonwealth points of contact within one hour of the incident, or immediately the next business day if the incident occurs after hours.

Trained and certified NSOC personnel, using the NMS, will prepare historical networks and system reports for the State 911 Department staff as agreed. The reports may be hourly, daily, weekly, monthly, or annual, and will include performance information for the following:

- Call counts by type, origination point, and destination PSAP
- Latency
- Jitter
- Packet loss
- Throughput
- Traffic volumes
- Up time
- Alarms received
- Descriptions of responses and resolutions

The NSOC will utilize a Security Information and Event Manager (SIEM) to collect security messages and alerts from all system devices, servers, and workstations as well as firewall logs. This will provide an integrated picture of the security status of the entire NG9-1-1 system in order to monitor, analyze, and remediate security incidents. More details describing the flow of security information are provided in Section 8.11, Security, Anti-Virus, and Patch Management.

All network performance monitoring tools proposed and used will be based on industry-standard software and platforms, as already proven and used by the GDIT team.

8.20.8. Training of Technicians

The contractor shall conduct training of all contractor technicians, including customer service technicians, specially trained technicians, field technicians, and regional supervisory service technicians, performing services under this contract, or any renewal thereof. Such training shall take place at regular intervals and shall include industry standard skill set testing. At the request of the State 911 Department, the contractor shall provide verification of such training to the State 911 Department. The contractor shall submit to the State 911 Department a comprehensive training plan, including without limitation, the training curriculum, and shall cooperate with the State 911 Department to correct deficiencies identified by the State 911 Department.

At the request of the State 911 Department, the contractor shall remove any and all technicians identified by the State 911 Department for reasons including, but not limited to, lack of or inadequate training or performance issues, from performing services under the contract, or any renewal thereof.

GDIT will comply with the RFR specification.

Upon award, GDIT will develop a comprehensive training plan for all GDIT team technicians to ensure regular training in industry-standard skill sets and also technology and applications specific to the proposed solution. This training plan and curriculum will be submitted to the State 911 Department for review and revision.

All technicians performing services under this contract will be trained, including help desk and customer service technicians, field technicians, and regional supervisory service technicians. GDIT's own Massachusetts-based training organization will develop the training plan and curriculum in concert with our teammates and OEMs, and the program office will retain training records for verification purposes, and will provide copies of the training materials if requested.

If requested by the State 911 Department, GDIT will remove technicians from performing on the contract for any reason, including performance issues or insufficient training.

8.20.9. Monitoring of Applications, Appliances, and CPE

The contractor shall monitor all applications and appliances located in the data centers as well as PSAP CPE from a centralized location, with a strong preference that the centralized location is within the Commonwealth. The contractor shall receive and monitor uninterruptible power supply alarms. The contractor shall ensure that all alarms shall also be received and monitored. The contractor shall have the capability of performing remote maintenance to further investigate alarms or restore alarms. The contractor shall monitor all ports, inbound and outbound, on the border control functions.

The contractor shall provide the State 911 Department with notification of software or equipment updates and modifications via a product change notice, technical service bulletin, or a new product announcement. The State 911 Department shall, in its sole discretion, determine whether the updates or modifications are required. If the State 911 Department determines that the product update or modification is required, the contractor shall provide the pre-release notification, including a step by step installation process that contains backup procedures of all critical data consisting of configuration settings, installation procedure and a back out procedure. Prior to deployment of new software upgrades or fixes, the contractor shall document that the required testing as described herein has been completed. Once the new product or modification is released, the contractor shall install the upgrade or modification/fix process at a dedicated facility, provided by the contractor, within the Commonwealth to trial the upgrade or modification/fix process. The contractor shall invite representatives of the State 911 Department to attend all aspects of the testing. If the testing cannot be accomplished at the dedicated facility, the State 911 Department shall select a training site for the testing. After testing of the upgrade or modification process has been completed and the results of such testing have been fully disclosed to the State 911 Department, the State 911 Department shall make a final decision as to whether to accept the upgrade or modification. If accepted, the contractor shall provide a proposed roll-out schedule for the upgrade or modification to the State 911 Department, and following approval of the schedule by the State 911 Department, shall begin the roll-out with the State 911 Department training sites followed by primary PSAPs. The contractor shall ensure that the step by step installation process referred to above is strictly adhered to at all sites.

In cases where a software issue is identified at a specific site where a code change is required, the contractor shall provide a pre-release notification. The contractor shall identify to the State 911 Department versions of firmware or drivers if there are specific modifications for that firmware or driver.

The contractor shall provide the State 911 Department with a standard change management document that will describe any software system or manufacturer default setting changes that are implemented by the contractor. The contractor shall promptly provide the State 911 Department with any and all updates to the standard change management document.

GDIT will comply with the RFR specification.

Remote monitoring of data center applications and appliances by the GDIT NSOC will include 24x7x365 centralized monitoring of alarms and reporting using SolarWinds management and reporting software tools. The team will use the ad hoc reporting and summarization of events and data that the tools make possible for diagnosing issues and performing detailed analysis.

CPE remote monitoring will use remote utilities developed by GDIT and our teammates for monitoring, diagnosing, troubleshooting, and repairing many of the errors known or unknown to a PSAP.

Remote monitoring includes the following services:

- 24x7 monitoring of all servers, workstations, LAN components, operating systems, application systems, and any other SNMP/IP compliant device on the network
- Alarm notification to first level support should an alarm threshold be exceeded
- Remote troubleshooting tools to diagnose hardware and software problems
- Performance monitoring of network and computer components
- Ability to take "remote control" of monitored workstations and servers to allow for real-time viewing and the ability to make system changes
- Network flow and performance monitoring, including threshold alarms
- Monitoring of uninterruptible power supplies/alarms
- Monitoring of all ports, inbound and outbound, on the border control functions

The 9-1-1 call processing equipment is absolutely mission-critical to the PSAP; without it call takers cannot perform their function. All systems will eventually fail without proper maintenance and management. However, some 9-1-1 CPE vendors built their monitoring systems as a loosely integrated afterthought. Add-on systems don't capture enough detail for troubleshooting or failure analysis. NG9-1-1 CPE diagnostics should be tightly integrated with – and included as part of – the CPE, monitoring should fine grained, and should capture enough detail to facilitate rapid troubleshooting and root cause analysis.

The GDIT team's proposed solution keeps PSAPs running by detecting problems before service disruption using a fully integrated, powerful, fine-grained monitoring system included in every 9-1-1 system. The system monitors thousands of variables by making dozens of specific checks along the following logical layers: network connectivity, hardware health, system security, resource availability, service availability, and application logs. The system automatically monitors all variables and will automatically alert the NSOC as necessary.

The GDIT team's CPE monitoring system generates emails on all alarm and recovery conditions, providing assurance that multiple levels of NSOC staff and management are aware of issues. Each email lists the monitored variable or subsystem and identifies the current status. The system monitors many items beyond what is available strictly with SNMP.

The GDIT team's solution provides fine-grained insight into and management of system-wide configuration, including hardware, services, and network components. The configuration management system provides centralized, XML-based, validated and version controlled configuration. The master configuration is retained in a version-controlled file store that provides Authentication, Authorization, and Accounting controls for all configuration changes. Therefore, only authorized technicians are allowed to make system-level configuration changes and all changes are timestamped and logged with a compulsory explanation. Individual changes are stored and tracked independently, allowing any single previous change or range of changes to be undone. The system configuration can also be reset to its prior configuration at any point in time in past.

Any software and equipment updates and modifications proposed or recommended will be formally reported in accordance with a standard change management document. Non-routine updates and modifications will first be tested in a GDIT team facility with test results provided to the State 911 Department for review and approval before incorporation into any live system. Commonwealth representatives will be invited to attend the testing.

GDIT's teammate DSS is already following a similar process. Generally, prior to release, a test environment is set up at a designated Training Facility at Taunton, Maynard, or Springfield; a set time for testing; then an incremental release plan to each of the PSAPs. DSS has State 911 Department–accepted Change Management and Acceptance Testing type documents currently in use.

If the change is approved, GDIT will develop a proposed rollout schedule for submittal to the State 911 Department for approval.

Any updates or modifications to the Master Change Management Document will be submitted to the Commonwealth in a timely manner.

8.20.10. Performance Monitoring

The contractor shall provide overall performance monitoring of the entire system as part of the initial warranty and any subsequent maintenance.

GDIT will comply with the RFR specification.

The proposed integrated monitoring capability includes not only failure and service availability monitoring, but performance monitoring as well. The system configuration includes tunable performance thresholds for processor, memory, and disk load along with other parameters. Each metric has associated warning and critical thresholds that will trigger notification of appropriate technical personnel at the NSOC. Performance monitoring of the entire system will be included as part of the provided warranty and ongoing maintenance.

8.20.11. Remote Diagnostics

The contractor shall provide remote diagnostics and maintenance that permits the contractor to monitor system performance, and perform routine diagnostics and maintenance from a remote maintenance facility, and bidders shall identify the location and capabilities of this facility.

The GDIT team's solution with its remote diagnostics capability reduces the need for on-site service calls (dispatches), eases maintenance, and improves support response time by providing access to all configurations remotely. All configurations are stored centrally on the CPE application servers. Individual device configurations are generated from a single master configuration file. The master configuration is version controlled and backed up daily. All configuration capabilities are controlled and managed at the NSOC, but they are accessible from anywhere on the private network, including the backup NOC and SOC facilities.

Remote support will be the primary path for issue investigation and resolution, leveraging a secure IP connection into the solution environment. With this, local technician support is often not required through controls, element management, and network management systems placed at the GDIT NSOC.

The GDIT NSOC is located at our existing facility in Needham, MA and is being custom-tailored to support the Commonwealth for this contract. GDIT has a 24x7x365 NOC located in

Fairview Heights, IL that will serve as the backup facility to the NSOC and will also provide Tier III/IV support. The in-place, proven processes and procedures at the Fairview Heights NOC are being used as a basis for the Massachusetts NSOC, but the capabilities of this new NSOC will specifically match the Commonwealth's requirements for this project.

8.20.12. Notification and Escalation

If a catastrophic system malfunction has occurred, the contractor shall generate a trouble ticket and shall notify the State 911 Department of the malfunction within fifteen (15) minutes of that determination by text message and group e-mail, or as otherwise directed by the State 911 Department. Within forty-eight (48) hours of the restoration of the catastrophic system malfunction, the contractor shall provide the State 911 Department with an Incident Report and shall provide in that Incident Report, (1) a root cause analysis of the event, an estimated date by which it will submit to the State 911 Department a root cause analysis of the event, or an explanation of why a root cause analysis is not possible, and (2) a plan to upgrade the applicable components at all operational PSAPs and or data centers with the necessary repair, or the estimated date that such plan will be submitted to the State 911 Department.

If the contractor has determined that a major system malfunction has occurred, it shall generate a trouble ticket and shall notify the State 911 Department of the malfunction within fifteen (15) minutes of that determination by text message and group e-mail, or as otherwise directed by the State 911 Department. The contractor shall, within forty-eight (48) hours of restoration, provide the State 911 Department with an Incident Report of the event. The contractor shall indicate in the Incident Report whether the major system malfunction is systemic, an isolated incident, or if it is unknown whether the event is an isolated incident or systemic and shall provide in that Incident Report, (1) a root cause analysis of the event, an estimated date by which it will submit to the State 911 Department a root cause analysis of the event, or an explanation of why a root cause analysis may not be possible, and (2) a plan to upgrade the applicable components at all operational PSAPs and or data centers with the necessary repair, or the estimated date by which it will submit such plan to the State 911 Department.

The contractor shall submit a notification and escalation path plan for catastrophic, major, and high priority system malfunctions in, at a minimum, the following periodic increments:

Restoration Phase

Immediate: The contractor shall determine whether a malfunction is catastrophic, major, or high priority, and shall, within fifteen (15) minutes of such determination, generate a trouble ticket that will include the date and time of such determination.

15-30 Minutes: Within fifteen (15) to thirty (30) minutes of the determination that a malfunction is catastrophic, major, or high priority, the contractor shall attempt to isolate the malfunction to a network, application and appliance or CPE issue, and shall determine and engage the appropriate resources to resolve the issue. In the event of a catastrophic malfunction, the contractor shall dispatch the appropriate resources, and at a minimum, a trained and qualified technician, to the data center within one (1) hour. The contractor shall dispatch resources to the PSAP and/or the data centers, and the contractor shall establish and provide, upon request of the State 911 Department and/or the PSAP, an estimated time of arrival of any required resource(s) at that location(s). The contractor shall track all related activity during this time period in the trouble ticket, including the status of any network troubles, that were referred. If the event is catastrophic, the contractor shall, within thirty (30) minutes of the determination, employ an internal notification process that will advise appropriate contractor personnel of the event.

30-60 Minutes: Within thirty (30) to sixty (60) minutes of the determination that a major system malfunction has occurred, the contractor shall provide a status update to the PSAP and the State 911 Department that shall include an updated estimated time of arrival of technicians, if applicable, as well as any known information. Within thirty (30) to sixty (60) minutes of the determination that a catastrophic system malfunction has occurred, the contractor shall establish an informational bridge with the State 911 Department to keep the State 911 Department informed of progress regarding restoration efforts.

60 Minutes plus through Restoration: For major system malfunctions, the contractor shall monitor the progress of the restoration process. If required resource commitments have not been fully committed with an expedited response, the contractor shall escalate the malfunction to the next level manager. At each half hour increment if required commitments have not been made, the contractor shall escalate the issue to the appropriate organizational level. For catastrophic system malfunctions, as required by the notification process described in the paragraph "15-30 Minutes" above, the contractor shall ensure that appropriate organizational management have been notified and

that appropriate resource commitments have been secured. For catastrophic and major system malfunctions, the contractor shall provide a status report to the State 911 Department and the PSAP at intervals of a minimum of every hour that shall include an estimated time of arrival of the technician(s) and shall include sufficient detail so as to permit the State 911 Department and the PSAP to appropriately employ the information set forth in the status report(s).

For catastrophic, major and high priority system malfunctions, the contractor shall track all related activity in the trouble ticket and the Incident Report. For catastrophic, major, and high priority system malfunctions, notification shall be provided via text message, group e-mail, and by any other means as directed by the State 911 Department.

Should the State 911 Department elect, during a major system malfunction or high priority system malfunction, to escalate/communicate an issue during any of the above time periods, the State 911 Department will contact the help desk. The help desk shall immediately transfer the State 911 Department to the appropriate manager who will handle the escalation request. If the appropriate manager is not available, the customer service center shall arrange a call-back to the State 911 Department from the appropriate manager within fifteen (15) minutes.

Should the State 911 Department elect, during a catastrophic system malfunction, to escalate/communicate an issue during any of the above time periods, the State 911 Department will contact the Contract Manager (as designated by the contractor) who will handle the escalation. The Contract Manager shall ensure that the State 911 Department escalation request is immediately addressed, and if necessary, shall arrange for a call-back to the State 911 Department from the appropriate manager within fifteen (15) minutes.

The contractor shall track and report on all activities from inception of the call to repair.

Post Restoration

Once the contractor determines that restoration is completed, the contractor shall:

- *Enter the review stage to determine whether failure has been permanently repaired. This stage shall include investigating the cause of the failure, and documenting and instituting change where necessary; and*
- *Provide the Incident Report, and upon request of the State 911 Department, the trouble ticket relating to the incident in the Incident Report, within forty-eight (48) hours of restoration in order that the State 911 Department can confirm restoration to the satisfaction of the State 911 Department. The State 911 Department may release such Incident Report to a PSAP or other interested parties upon request of such PSAP or other interested parties consistent with any applicable public records laws and regulations.*

GDIT will comply with the RFR specification.

GDIT manages escalation and subsequent resolution through our highly configurable and widely deployed incident management framework. Providing the traceability and systematic notification of support personnel is GDIT's Remedy trouble ticket system.

GDIT's Remedy trouble ticket system is already customized to enable the sending of text messages and notification emails when certain classifications of troubles are reported. As soon as a trouble ticket is opened and classified as catastrophic, major, or high priority, text messages and emails will be sent immediately to the Commonwealth and to key members of management on the GDIT team.

When malfunctions reported in catastrophic and major tickets are restored, GDIT will develop and deliver an Incident Report within 48 hours. The Incident Report will include a root cause analysis (or provide an estimated date when the root cause analysis will be provided, or an explanation of why a root cause analysis may not be possible). For major malfunctions, the Incident Report will also state whether the malfunction was systemic or an isolated incident (or unknown).

The following timeline will be followed for processing and reporting on catastrophic, major, and high priority tickets. A summary of the notification and escalation flow is shown in Figure 92.

- **Within 15 minutes of the report:** Determine the classification of the malfunction. Emails and text messages will be sent immediately to the Commonwealth and to appropriate GDIT team personnel.
- **15 to 30 minutes:** Troubleshoot and isolate the issue to be a network, application, appliance, or CPE problem. Determine resources necessary to resolve the issue and dispatch the appropriate personnel.
- **30 to 60 minutes (Major):** Provide a status update to the PSAP and the State 911 Department updating estimated time of arrival of technician(s) and any other pertinent information.
- **30 to 60 minutes (Catastrophic):** Establish an informational bridge with the State 911 Department to keep the Commonwealth informed about status and progress of restoration activities.
- **60 minutes through restoration:** For major malfunctions, escalate after 30 minutes if required resources have not been committed. For both catastrophic and major tickets, provide a status report to the State 911 Department and the PSAP at intervals of an hour or less. The status report will include details of restoration efforts and plans, including updated Estimated Time of Arrival (ETA) of dispatched personnel. All details of the restoration activities will be tracked in the ticket and included in the Incident Report.
- **Post restoration:** The review stage begins, and the GDIT team will determine whether the malfunction has been permanently repaired. The review stage also includes an investigation of the cause of the failure, and documenting and instituting preventive changes where necessary. The Incident Report is delivered to the Commonwealth.

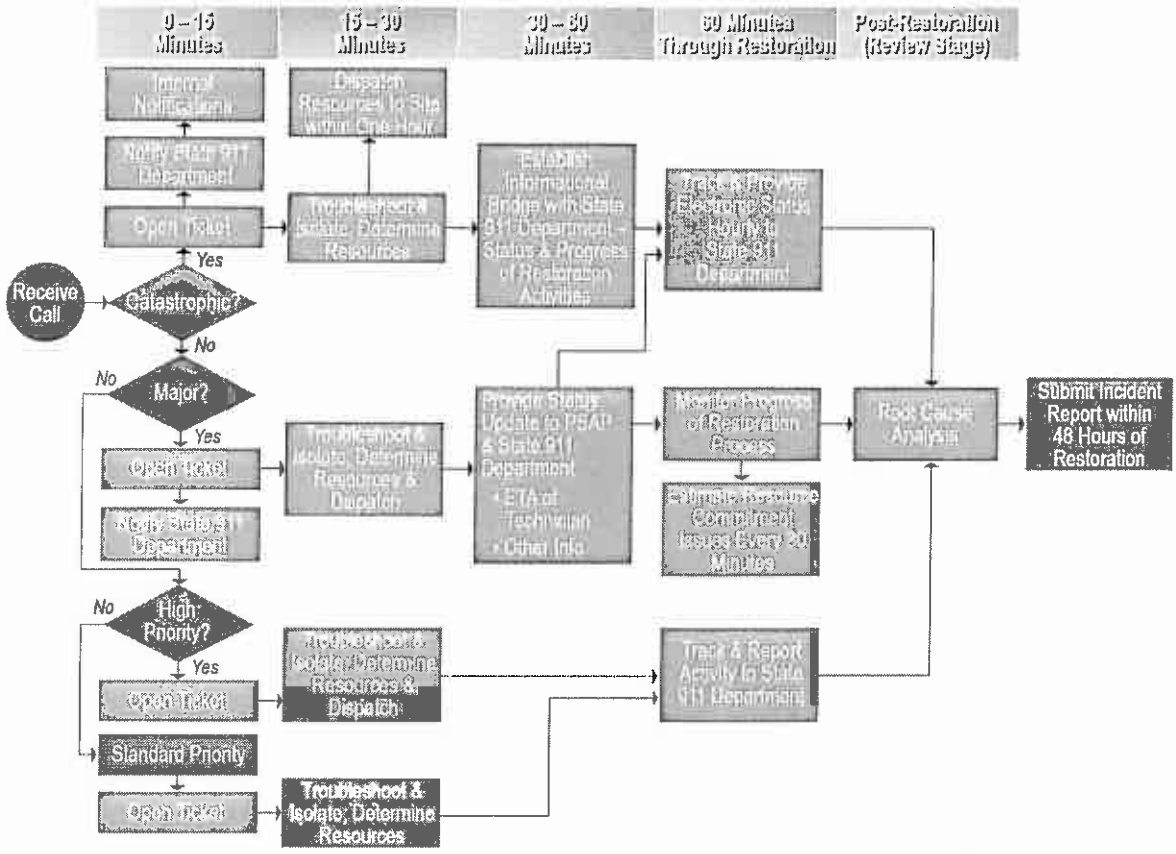


Figure 92. Notification and Escalation Timeline

Additional triggers and timelines for automatic notification can be added as desired by the Commonwealth.

If the Commonwealth calls the help desk regarding a major or high priority ticket, the help desk will immediately transfer the call to the responsible manager or arrange a call back within 15 minutes. If the Commonwealth calls the Contract Manager to escalate a catastrophic ticket, the Contract Manager will ensure immediate escalation and will arrange a callback within 15 minutes, if requested.

8.20.13. System Malfunction

In the event of a catastrophic system malfunction or major system malfunction, whether due to circumstances covered under warranty or maintenance agreement, or due to Acts of God or nature, or any other cause, the contractor shall have a replacement system readily available, which can be installed and operational within forty-eight (48) hours.

GDIT will comply with the RFR specification. The Disaster Recovery Plan outlined in Section 8.11.7 (Disaster Recovery/Business Continuity) will be implemented in the event of a catastrophic system malfunction.

The CPE configuration management infrastructure proposed allows any customer system or component to be completely reinstalled and reconfigured automatically within minutes. An entire

customer solution can be automatically re-provisioned from new in the box, bare metal components within hours. This is due to the fact that all configurations of all servers, processes, and network devices are centrally managed and distributed; no component of software or hardware is ever manually configured.

Spare hardware will be maintained in the Commonwealth to rebuild the solution as necessary. With the automated provisioning system, the system will be easily rebuilt in a deterministic fashion to its previous configured state in less than 48 hours.

8.20.14. System Backup and Restoration Capability

The contractor shall provide the necessary equipment (hardware and software) to allow for required backups and/or restoration of system applications and appliances, including for payload and user information. The contractor shall provide a comprehensive backup solution that is expandable and that includes detailed monitoring. Bidders shall state the estimated time to restore event logs and event recording. Bidders shall explain in detail how the backups/restorations are accomplished and what effects these operations have on the production environment. Systems that require the system to be removed from service or placed into a degraded mode of operation for routine backups will not be acceptable. The system backups shall be performed without State 911 Department or PSAP intervention. Bidders shall identify the frequency of routine backups. The system shall automatically prepare a listing of all information manually deleted from the system and of all information automatically moved to archives or purged.

The contractor shall maintain current images of the servers and workstation.

The contractor shall ensure that the system archives system information for such period of time as required by law, or as otherwise required by the State 911 Department.

GDIT will comply with the RFR specification.

The GDIT team understands large and complex integrated system deployment and management. With large systems that have many diverse hardware and software components, configuration and tuning of the system can be a time-consuming exercise. When a server or other hardware needs to be replaced, it is critical that the device can be restored to the exact configuration of the failed unit. This restoration must include the complete final state of all: hardware, firmware, software, patches, configurations, and historical data. This problem is much further complicated when using COTS equipment from different vendors who support diverse interfaces and formats for device configuration. In the event of a catastrophic failure, it is critical to have the ability to rebuild the complete integrated solution (including outlying networked components) as quickly and reliably as possible.

Common image-based solutions are 'easy' at first glance, but realistically are fraught with many problems. With a system restoration strategy based on imaging, heavyweight snap shots of all system binary, configuration, and user preference information are captured. For a true one-touch restoration, a new image must be created each time any software update or configuration change is made. Further, a different image is required for each possible system configuration. This leads to an exponential explosion of images which are difficult to store, manage, and retrieve when needed. Practically, this leads to creation of one or more 'lowest common denominator' images that must be applied along with a manual – and error-prone – re-configuration process. Further, remote and network devices are difficult or impossible from which to create images or restore images.

The GDIT team's approach eliminates problems with a proliferation of image versions and image staleness while also providing much more fine-grained configuration state capture than is available with system images.

We will provide a complete, automated, end-to-end solution for software, configuration, preference and historical data capture, management, and deployment. Firmware, software, system configuration, and user preferences have different characteristics and need to be managed using appropriate tool, not a one-size-fits-all solution. In our CPE system, there are four integrated mechanisms for system configuration management. First, software and firmware are managed at a functional package level by a centralized software update and dependency manager. Second, system configuration is centrally managed in a validated and version controlled manner. Third, point-in-time snapshots of user preferences and historical data are captured nightly. Finally, historical data and payloads such as recordings and images are replicated in real-time between data centers. The combination of these solutions allows the complete rebuild from bare metal to a fully functional system with historical data in a matter of minutes, not days.

The system will automatically prepare and archive a listing of information deleted, moved, archived, or purged. All system archives will be maintained for the time period required by law and/or the State 911 Department.

Software Update and Dependency Management

The systems can be updated or completely rebuilt fully automatically with exact precision. The automated provisioning system generates and manages software and configuration images for services and devices solution wide. The provisioning system automatically generates, loads, and updates device and service configuration files. It also manages software updates including dependencies between packages and versions across the solution. Device software and configuration is served to network devices via HTTP and FTP.

The software management system is tightly integrated with the provided customized Linux distribution and manages software revisions and configuration for every component of the system, including non-server networked equipment. The system provides complete and accurate fully automated installation and configuration of any customer server.

The software management system provides additional security by cryptographically verifying a package's source is authentic and the contents have not been tampered with or accidentally corrupted. Each individual software package is cryptographically signed to ensure the origin of the package and that the contents have not been modified. Within each package, each file has a cryptographic fingerprint so that the complete state of the system can be verified at any time.

Data Replications and Backups

The backup system provides multiple layers of data replication and redundancy. Real-time replication is performed between the two servers in each cluster for all types of data, including: system-generated historical data, user preferences, and bulk data such as images and recordings. The same data is asynchronously replicated across data centers between clusters in a super cluster. Lastly, point-in-time snapshots of historical data and user preference data are captured nightly and exported to external network storage. Nightly backups including schema information

are included in standard SQL Data Definition Language (DDL). This backup may be used to restore the database to an external system.

8.20.15. UPS Maintenance and Monitoring

The contractor shall provide, maintain, and monitor UPS. The contractor shall perform preventative maintenance, including recommended firmware updates, load testing, as well as battery testing and replacement, on all UPS. The contractor shall monitor the UPS using SNMP traps via the existing Ethernet network interface card installed in the UPS.

GDIT will comply with the RFR specification.

The GDIT team will maintain and monitor all UPS systems deployed in the solution. The NSOC will monitor each UPS using SNMP traps via the existing Ethernet network interface card installed in the UPS. Regular preventive maintenance will be performed by our dispatch technicians, including firmware updates, load testing, and battery testing. Batteries will be replaced when required.

GDIT has DC power engineers on staff who have successfully supported power system problems and outages for the U.S. Air Force, the FAA, and other customers. They are available for remote consultation and/or dispatch to a site.

8.20.16. SNMPv3 Support

All IP manageable network hardware shall support the SNMPv3 specification for performance monitoring via standard management information base objects and secure remote management to require SSHv2 on devices that can be remotely managed.

GDIT will comply with the RFR specification.

IP-manageable network hardware equipment selected for the overall GDIT solution, including data center hardware, currently provides the capability to be monitored remotely at our NSOC via SNMPv3, or the OEM will implement that capability as a product upgrade.

The CPE system includes a tightly integrated monitoring and alerting platform. This platform gathers a large amount of fine-grained performance and availability data through a variety means. Much of this data is gathered through standard SNMP interfaces from COTS equipment. However, the monitoring system also gathers information – which are not available via SNMP – through other interfaces such as IPMI, ICMP, and SSH.

The alerting system generates emails on all alarm and recovery conditions. Each email lists the monitored variable or subsystem and identifies the current status. The monitoring solution includes a variety of alarm states some of which are purely informational. Fault conditions of all types are recorded in log files.

8.20.17. Preventive Maintenance

The State 911 Department requires regular preventive maintenance to preclude failures due to lack of maintenance. The contractor shall supply a schedule of preventive maintenance work for the duration of the contract, including renewals, indicating what work is to be performed, where the work will be done and the times when the work will commence and end. The written approval of the State 911 Department is required prior to commencement of work involving preventive maintenance on any application or appliance which, if a catastrophic failure were to occur, could result in a cascading failure of the system.

Bidders shall describe in detail its preventive maintenance program. Bidders shall specify the preventive maintenance schedule and/or the maintenance steps and shall estimate the amount of scheduled maintenance (system down-time) for each component of the system. This preventive maintenance shall include system health and pro-active monitoring. The maintenance windows shall be by mutual agreement of the parties.

The contractor shall perform routine, preventive maintenance on the system. The contractor shall perform such maintenance according to the plan and schedule approved by the State 911 Department. The contractor shall provide written documentation of the results of the preventive maintenance to the State 911 Department.

Maintenance shall include keeping all system and equipment software up to date. At the end of the warranty period, all software shall be of the latest version, release, and service release that applies to the equipment provided that has been authorized by the Department.

GDIT will comply with the RFR specification.

GDIT has established procedures to identify actual and potential defects, nonconformities, and methods for improvements in our processes and to correct and prevent future recurrence. These procedures provide a mechanism for reporting, documenting, and managing current and potential problems that adversely affect quality to ensure rapid and effective resolution.

Preventive action includes review and analysis of all information sources to detect and eliminate potential problem procedures or processes. "Lessons learned" are collected at various stages throughout a program or project's life cycle and are evaluated to determine what changes should to be made in an effort to achieve continual improvement.

Our comprehensive preventive maintenance approach includes 1) the creation of maintenance schedules; 2) performing system inspections and required maintenance; and 3) conducting monitoring activities. Our preventive activities minimize remedial maintenance actions and ensure system availability is not compromised by neglecting routine health maintenance tasks.

Creation of Maintenance Schedules. We will pre-load scheduled maintenance actions into the Remedy ticketing system to automate the process of generating preventive maintenance tickets at the required intervals. This reduces the chance of accidentally missing a required PM action. We will coordinate through the respective customers to ensure that a scheduled maintenance activity aligns with the site's schedule and to schedule authorized maintenance windows.

Performing System Inspections and Required Maintenance. We implement regularly scheduled maintenance updates, patches, cleaning, and performance improvements as recommended by the OEMs and in accordance with both GDIT and industry best practices.

As part of our preventive maintenance approach, the GDIT team will continuously assess system functions to proactively address performance issues. This includes engineering activities to insert alarms and notifications in the monitoring applications for specific system degradation criteria.

Performing Monitoring Activities. NSOC monitoring of the devices and systems is a key component of our overall preventive maintenance activities serving to identify system abnormalities often well before a particular component fails. To perform this routine monitoring we use tools such as SolarWinds. Using monitoring tool system performance logs we perform trend analyses to proactively identify, isolate, and mitigate problems before failures have the opportunity to occur, or before they can develop into major defects.

8.20.17.1. Preventive Maintenance Tasks

The contractor shall perform the following preventive maintenance tasks for all workstations and servers on a schedule recommended by the equipment manufacturer, but such preventive maintenance shall occur no less than twice per year:

Cleaning: The contractor shall clean all PC's and servers based on the equipment manufacturer's recommendation and at a minimum shall include vacuuming dust and dirt from all fans, intakes and drive devices. All PCs and servers shall be opened to clean inside each unit. Prior to commencement of work, the contractor shall provide a listing of sites to be visited during a particular month to the State 911 Department. The contractor shall develop a checklist/form detailing the items addressed during the scheduled preventive maintenance and shall, upon completion of the maintenance, deliver the completed checklist/form to the State 911 Department verifying that this maintenance was completed.

Disk Optimization: The contractor shall perform disk optimization on all workstations automatically via installed software and performed continuously.

Through remote monitoring, the contractor shall ensure that it manages alerts which will identify the percentage of disk space utilization. Where alerts are received respective to disk space allocation, the contractor shall ensure that it will analyze the associated disk drive and work to identify a solution.

GDIT will comply with the RFR specification.

Preventive maintenance for all deployed workstations and servers will be scheduled at least twice per year and more often if recommended by the equipment manufacturer. Specific examples of preventive actions by our team include but are not limited to:

- Preparation and submittal of preventive maintenance checklists
- Internal cleaning of servers and workstations
- Disk optimization
- Patch management
- Monitoring of threshold alarms
- Monitoring of bandwidth usage and availability in order to identify bottlenecks in the system
- Responding to real-time HVAC alerts for temperature, humidity and other environmental conditions before they reach critical levels

Disk space utilization will be monitored remotely. When percentage thresholds exceed preset levels and alerts are generated, the NSOC will analyze the drive and determine the solution required.

8.20.18. Spare Equipment Repair and Replacement

Bidders shall describe the policy for expediting repair of equipment that has been inoperative for eight (8) hours, twenty-four (24) hours, and longer than twenty-four (24) hours.

A sufficient supply of spare parts shall be maintained at various locations within the Commonwealth to allow immediate restoration of operation of the system. In the event that these parts are consumed, replacement stock shall be available via emergency request and airfreight within twenty-four (24) hours of the equipment failure.

Stocking of spare parts shall remain the sole responsibility of the contractor.

GDIT will comply with the RFR specification.

The GDIT Help Desk and NSOC will track and manage trouble tickets to expedite the restoration of equipment and systems. When a ticket has been open because equipment has been inoperative for eight hours without resolution, the Remedy trouble ticket system will automatically notify (via email and text) the Help Desk Manager and NSOC Manager so that additional steps may be taken. Automatic notification and escalation to additional management personnel will occur at 24 hours and at 8-hour intervals beyond 24 hours.

If needed spare equipment is not available to the dispatch technician due to multiple failures or other unforeseen circumstances, the GDIT team will work to deliver spares from another depot within the Commonwealth or via expedited shipping.

The GDIT team will stock and stage spare parts and equipment at multiple locations in the Commonwealth to ensure rapid deployment when replacements are required for malfunctions.

The GDIT NSOC and our dispatch technicians will coordinate the return and restocking of spare and replacement parts and equipment. We have developed and refined logistics and material handling processes and procedures that ensure efficient and rapid processing of replacement hardware. These in-place procedures will be tailored and adapted to the Commonwealth's specific requirements for this project. Working with our partners and vendors, we already have procedures and capabilities in place to overnight parts when required within twenty-four (24) hours of the equipment failure, and even to ship air freight counter-to-counter same day for emergency response.

8.20.18.1. Spare Inventory at Contractor Locations

The contractor shall maintain a level of spare inventory that is consistent with the needs of repair. The contractor shall, on a monthly basis, track and analyze equipment failures at data centers and PSAPs that require a replacement from spare inventory. The contractor shall adjust the inventory as needed based upon a monthly analysis. Analysis shall be documented and provided to the State 911 Department upon request.

The contractor shall maintain remote parts depots located at various contractor locations throughout the Commonwealth. The contractor shall establish inventories at these locations that shall include, but not be limited to: workstations, monitors, keyboards, mice, devices, patch cables, telephones sets, critical server and network components, power supplies, Ethernet switches, and other necessary hardware or peripherals. The contractor shall provide an inventory and location of each spare parts depot to the State 911 Department upon request. The contractor shall identify the model number and serial number of the spare parts.

The contractor shall maintain spare parts inventory at locations throughout the Commonwealth. The contractor shall identify such spare parts on Attachment N- Types of Spare Inventory to be Maintained at Locations Throughout the Commonwealth. The contractor shall use the spare inventory to support the data centers, PSAPs, and training centers and shall be adjusted and add to the inventory on an as needed basis. The contractor also shall use the inventory to replenish the remote parts depots when their stock becomes depleted due to repairs. If there is a repeated malfunction or failure, the State 911 Department may require the contractor to increase its spare parts inventory to ensure sufficient inventory is available to address this repeated malfunction.

GDIT will comply with the RFR specification.

The GDIT team will maintain spares depots at GDIT and partner locations across the Commonwealth, with inventories sufficient to support routine service restoration requirements. The inventory levels will be tracked and analyzed each month, and inventory levels will be adjusted upward when needed based on usage and State 911 Department requirements. This analysis will be documented and can be provided to the State 911 Department when requested.

Upon award, we will identify the spares for each location and submit Attachment N – "Types of Spare Inventory to be Maintained at Locations Throughout the Commonwealth." An initial spares list is provided in Attachment N of our proposal. These parts depots will be strategically located at our team's facilities throughout the Commonwealth, providing close and convenient access to the spare parts when needed at any site.

Spares stocked will include workstations, monitors, keyboards, mice, devices, patch cables, telephones sets, critical server and network components, power supplies, Ethernet switches, and other necessary hardware and peripherals. This spare parts inventory will support the data centers, PSAPs, and training centers. Inventory levels will be maintained and adjusted as needed. We will increase spare parts inventory if requested by the State 911 Department due to multiple malfunctions or failures.

8.20.18.2. Spare Inventory at PSAPs and Data Centers

In addition to the spare inventory that will be maintained at the contractor's locations throughout the Commonwealth, the contractor shall maintain critical spare inventory on-site at each PSAP and data center location. The contractor shall identify critical spare inventory that shall be maintained on-site at each PSAP on Attachment O- Types of Spare Inventory To Be Maintained at PSAPs. The contractor shall identify the critical spare inventory maintained on-site at each data center on Attachment P- Types of Spare Inventory To Be Maintained at Data Centers. The contractor shall add equipment to this list based on the frequency and type of repair so as to ensure that critical spare inventory is maintained on-site at PSAPs and data centers at all times. If there is a repeated malfunction or failure, the State 911 Department may require the contractor to replenish spare parts inventory.

GDIT will comply with the RFR specification.

The GDIT team will maintain a stock of critical spares for each PSAP and data center facility. Upon award, we will identify the inventory for each site and submit Attachment O – "Types of Spare Inventory To Be Maintained at PSAPs." Critical spare inventory will be maintained at each data center and will be identified on Attachment P – "Types of Spare Inventory To Be Maintained at Data Centers." Initial spares lists are provided in Attachment O and Attachment P of our proposal.

Equipment will be added to the inventories and noted on the lists as required based on frequency and types of repair. GDIT will replenish or increase spare parts inventory if requested by the State 911 Department due to multiple malfunctions or failures.

We will not only provide spares for PSAPs, but we will leverage our vast network of facilities and teammates in state, and proactive maintenance processes, to minimize on-site inventory required for PSAPs with space constraints.

8.20.19. Repair and Service Facilities

Bidders shall include a description of their service facilities, the size and qualifications of its staff, the number of years in business, and a list of customers (with names and telephone numbers) who operate systems of similar size and complexity for whom installation and maintenance services are performed. This information is required to demonstrate to the State 911 Department that the contractor is capable of installing, optimizing, and maintaining the system.

GDIT will comply with the RFR specification.

GDIT employs over 21,000 engineering, technical, and professional staff personnel in all 50 states delivering IT services and enterprise solutions serving federal, state, and local government customers.

All implementation and service activities will be initiated, managed, and tracked from GDIT's Center of Excellence facility in Needham, MA. This facility has office space for hundreds of employees, warehouse space for receiving and staging equipment and spares, and labs to fully support design, implementation, and maintenance activities.

Details of the GDIT team facilities, staff qualifications, and currently supported customers, including contact names and telephone numbers, are provided in Section 9, Bidder Qualifications. We have successfully installed, optimized, and maintained networks and systems of similar size and complexity for a variety of customers, including federal agencies and departments with hundreds of facilities across the country and around the world.

GDIT has partnerships with numerous Commonwealth-based IT and telecommunications firms employing trained and qualified technicians who are located within a one-hour driving distance from every identified PSAP and who have secure facility space for staging of spares. GDIT retains responsibility to ensure the local technicians are fully trained and capable of ensuring the highest level of systems performance and function. All technicians are supported by both GDIT and vendor subject matter experts for escalation and collaboration. We have successfully used this collaborative support model for many customers to rapidly troubleshoot and resolve problems, with NSOC, partner, and OEM subject matter experts providing remote support to on-site technicians via telephone and video tools such as FaceTime. Locations of the team's technicians are shown in Figure 93.

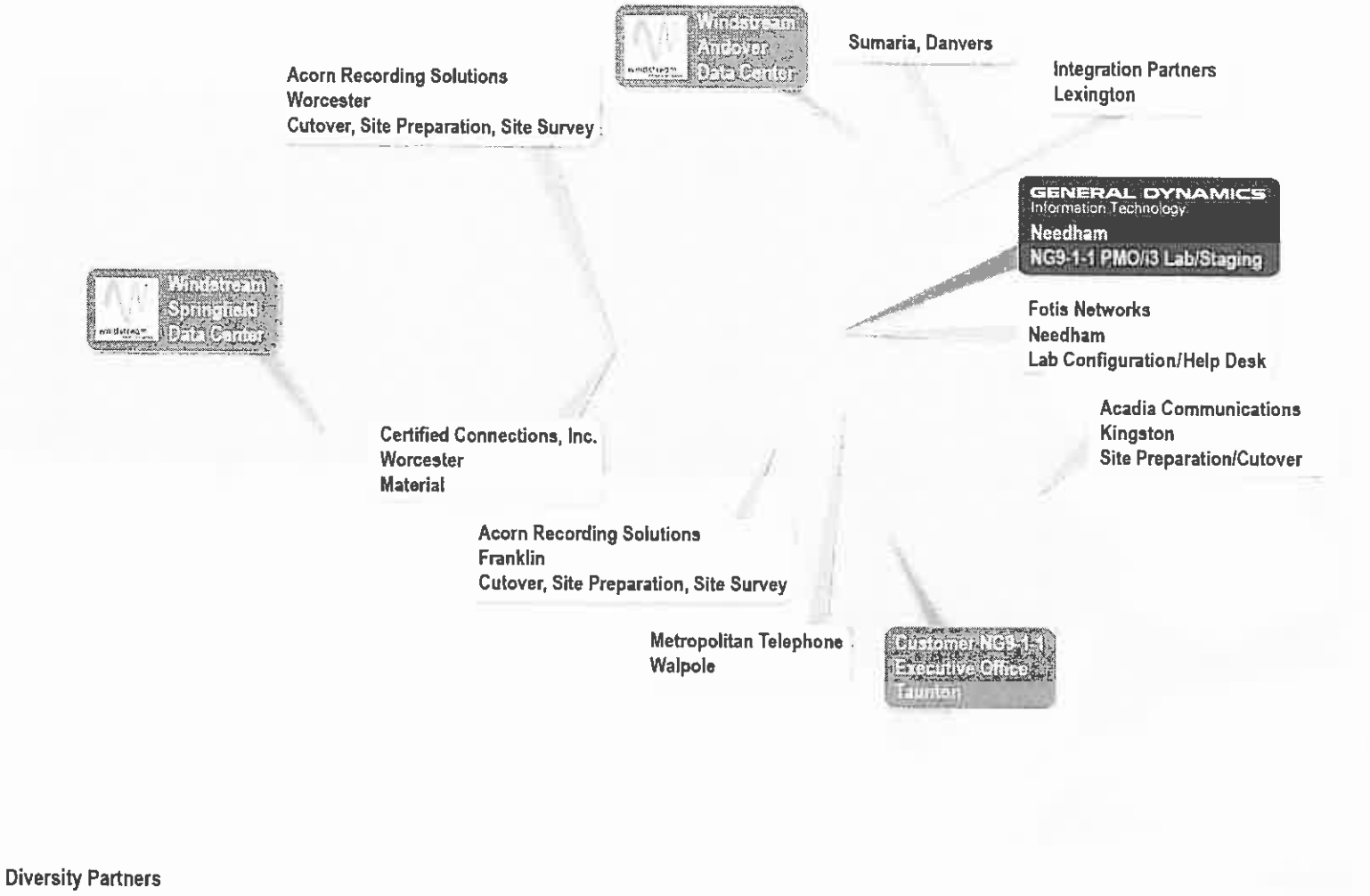


Figure 93. Locations of GDIT Team Technicians

In addition to the five dedicated GDIT Regional Supervisory Technicians able to quickly deploy to all PSAP and data center locations in the Commonwealth, the GDIT team includes small business partners for dispatches to locations around the Commonwealth, as well as our circuit (LEC) partner Windstream for resolving network issues (shown in Table 32).

Table 32. Maintenance Coverage Area – Massachusetts Counties

Teammate	Essex	Suffolk	Middlesex	Norfolk	Plymouth	Bristol	Barnstable	Duke	Nantucket	Worcester	Hampshire	Hampden	Franklin	Berkshire
Acadia Communications, LLC	X	X	X	X	X	X				X	X	X	X	X
Acorn Recording Solutions, Inc.	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Fotis Networks, LLC	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Metropolitan Telephone	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Sumaria	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Windstream	X	X	X	X	X	X	X	X	X	X	X	X	X	X

8.20.20. Maintenance of Contractor-Furnished Software

The contractor shall maintain all contractor-furnished software in a reliable operating condition, and incorporate the latest software changes applicable to the installed system to include version upgrades. The contractor shall describe the nature of his software maintenance coverage and program for maintaining reliable, efficient, and current software.

The maintenance service fee shall include providing and installing any system software patches, upgrades, enhancements, etc., developed by the software manufacturer during the service contract period.

GDIT will comply with the RFR specification.

All GDIT-furnished software will be maintained in a reliable operating condition and will include the latest software changes and version upgrades.

All contractor-furnished software maintenance activities will be controlled from GDIT's Needham Center of Excellence, with the extensive lab and integrated environment for testing and version control throughout the contract period of performance.

GDIT, as the system integrator, will manage each software iteration from subsystem providers, the respective independent versioning, system-level versioning, and management of subcontractor-specific software release processes. This integrated approach minimizes the Commonwealth's risk and exposure throughout the life cycle; software remains reliable and up to date through an integrated and system-oriented process.

The GDIT team's warranty and maintenance coverage includes continual updates and upgrades of software to ensure the integrity of operational systems. This maintenance is scheduled and performed in collaboration with, and with approval of, the State 911 Department. GDIT will provide the Commonwealth with visibility into the risk, impact, and reasons for such maintenance, with recommendations for applying the maintenance patches and upgrades in a manner that best meets the requirements. Typically, such maintenance is performed remotely, leveraging the redundant nature of systems to ensure no impact to services. Where on-site maintenance is warranted, GDIT will coordinate the schedule with the State 911 Department.

For the critical CPE solution software, team member Emergency CallWorks will work closely with the Help Desk, NSOC, and on-site technicians for all monitoring and maintenance issues.

The maintenance service fee will include the provision and installation of system software patches, upgrades, and enhancements developed by the software manufacturer throughout the service contract period.

8.20.21. Electrostatic Discharge Precautions

Any and all service technicians of the contractor working on applications and appliances or CPE shall follow industry standard electrostatic discharge precautions. Precautions shall include, but are not limited to, wearing protective boots straps and/or wrist straps and utilizing anti-static mats.

GDIT will comply with the RFR specification.

GDIT has a formal Quality and Environmental Health and Safety (QEHS) program that mandates Electrostatic Discharge (ESD) precautions for its employees, teammates, and subcontractors. All members of the GDIT team working on applications, equipment, or CPE will follow industry standard electrostatic discharge precautions that are mandated in our procedures, including the use of protective wrist straps or boot straps and anti-static mats.

8.21. ADDITIONAL SERVICES

At the request of the State 911 Department, the contractor may be required to provide additional services. The contractor shall complete the requested services through a separate statement of work to be negotiated by the parties at the time of request and subject to the terms of this RFR and any and all rates identified on Attachment E- Cost Tables. The cost tables are intended to capture all known commodities and services that may be needed as of the date of release of this RFR. Should the State 911 Department identify a need for a commodity and/or service within the scope of this RFR, but for which a rate was not requested on Attachment E- Cost Tables, bidders are advised that all rates shall be reasonable and consistent with that available in the industry.

GDIT will comply with the RFR specification.

Services and products that the Commonwealth may want to consider having GDIT implement as an additional service, per the definition in the RFR, are the following:

- **Rave Mobile Safety's Smart911 product**: As a hosted web-based application, Smart911 allows citizens to access a free secure web-portal, where they can provide critical information about themselves, members of their household, frequented addresses, emergency contacts, vehicles and pets, and associated communications devices. The citizen's Smart911 profile is displayed to telecommunicators whenever the citizen places a 9-1-1 call through a registered device. Smart911 is a national database. By adopting Smart911, Massachusetts PSAPs will have access to all Smart911 profiles, extending their reach beyond residents of the Commonwealth of Massachusetts to include any Smart911 registrant who uses a mobile phone within the geographic area supported by Massachusetts PSAPs. The national reach of the Smart911 database allows Massachusetts to not only better serve its own citizens, but any Smart911 registrant traveling to or through the Commonwealth.
- **ECW IP-Based NG9-1-1 Communication and Dispatch System**: DispatchStation® provides centers with the total capability of the standard CallStation and combines that with integrated dispatch capability found in many stand-alone CAD systems. Call taking and Dispatch is available directly from the Map with the support of traditional and

NG9-1-1, Mapped ALI and CAD features in one smooth workflow and reporting system. DispatchStation is provided with two (2) additional applications as part of the capability, AdminiStation and DecisionStation for complete call to event close dashboard reporting and data mining. One of the primary goals of the ECW platform is to streamline the effort of the typical call taker/dispatcher to truly integrate the processes such that a single application could be deployed and managed to work the way the centers actually do, by taking calls, mapping those calls and dispatching and managing resources in a much simpler and inexpensive manner.

- **EMC VMware** virtual desktop is a solution architecture that provides continuous availability of desktops, applications, and across devices, locations, and networks. It delivers virtual desktop sessions that follow end users across devices and locations. VMware View Security Server enables secure access to virtual desktops without the need for a traditional Virtual Private Network (VPN) solution. Alternatively, it can also be integrated with an agency's existing VPN solution. Deployment of a virtual desktop environment, depending on the application and degree of deployment, can have considerable operations and maintenance savings – oftentimes more than offsetting investment in licenses and or the minimal hardware required to support a virtual desktop.

- **GDIT University Web-based Learning/Training Solutions:** As the State 911 Department is expecting such a large number of students, GDIT recommends a couple of blended training solution options. The first option would be to convert all lower-level training to self-paced web-based modules that can be incorporated into the conversion ILT curriculum, so that the time spent in the classroom is devoted to higher-level learning and practice. Lower-level training is defined as foundational instruction, such as basic system concepts and definitions. In other words, the foundational knowledge would be taught through an online self-paced mechanism before students attend classroom sessions, and classroom sessions would be focused solely on applied learning. The benefits of this approach are multiple. For example, the foundational module(s) can be taken anytime and anywhere using Internet access. Individuals can learn at their own pace and around their own schedules, and this approach is significantly less expensive. A blended approach can reduce the number of foundational learning objectives taught in a classroom by 100%, as well as eliminate any training bottleneck that could occur when a class is limited to a maximum number of students per session.

  Another option would be to establish a virtual university. This online university is a virtual learning environment where classroom sessions could be delivered via a live synchronous environment. Instructors would be able to schedule online sessions and use the various interactive features such as whiteboards, videos, and chats. The virtual university concept would require the installation of an open source Learning Management System (LMS). This system allows for large student registration and throughput. The virtual university concept also allows for blended delivery of training where a course can include some self-paced online modules followed by live virtual class sessions with an instructor. GDIT recommends the implementation of an LMS to alleviate costs associated with ILT training implementation at multiple locations. This solution will also ensure consistent delivery of up-to-date training, and this would be especially useful for training associated with any system's updates.

8.22. REMOVAL OF CPE, APPLICATIONS, AND APPLIANCES

At the request of the State 911 Department at the termination or expiration of the contract, the contractor shall de-install and remove all CPE, applications and appliances furnished hereunder, including without limitation, servers, cabling workstations, interfaces, etc. to be stored in a location on-site at the PSAP or at such other location to be designated by the State 911 Department.

GDIT will comply with the RFR specification.

Upon State request, GDIT will de-install and remove all legacy 9-1-1 CPE, hardware, and cabling from the transitioned PSAP within ten (10) business days of the site acceptance date. GDIT will notify the State 911 Department upon completion of the de-installation effort and will work with the Department to store the removed hardware in a location(s) as directed. Should there be a requirement to pack and transport deinstalled CPE to locations other than the PSAPs, we will coordinate the work with the State 911 Department.

8.23. COMPLIANCE WITH AMERICANS WITH DISABILITIES ACT

All goods and services provided by the contractor shall comply with the Americans with Disabilities Act. The contractor shall be responsible for all modifications to hardware, software, or CPE as may be requested by a PSAP and/or the State 911 Department to ensure compliance with the ADA.

The contractor shall coordinate with the State 911 Department in the identification of all prospective attendees at contractor training(s) who require accommodation, and shall cooperate with the State 911 Department in its provision of such accommodation.

All technical and user documentation and any additional training material delivered by the contractor shall include alternative keyboard commands that may be substituted for mouse commands. Any documentation delivered under this Agreement and wholly owned by the State 911 Department shall be in an agreed-upon editable format.

GDIT will comply with the RFR specification.

GDIT has a long history of developing accessible training, or Section 508 compliant training for a variety of customers including Defense Acquisition University (DAU); eArmyU; the Morale, Welfare, and Recreation Academy (MWR) of the U.S. Army; Veterans Health Administration (VHA); Veterans Benefits Administration (VBA); the U.S. Postal Service; and the Naval Education and Training Command (NETC).

GDIT's involvement with Section 508 compliance began as early as 1999 when we were selected by the General Services Administration (GSA) and the Access Board to provide technical assistance to individuals and federal departments and agencies regarding the requirements of Section 508. To support this effort, GDIT developed instruction that is still available on U.S. government servers at: http://section508.gov under "508 Training." Since then GDIT has developed Section 508–compliant training for a variety of modalities such as web-based training, Instructor-led Training, and electronic and paper documentation.

GDIT will proactively coordinate with the State 911 Department to identify prospective attendees who may be hearing impaired, have visual disabilities at various degrees, or have psycho-motor disabilities. GDIT will provide alternate options as needed.

8.24. COMPLIANCE WITH INFORMATION TECHNOLOGY DIVISION ACCESSIBILITY STANDARDS

The contractor shall ensure that all deliverables adhere to (1) the Section 508 Standards for Electronic and Information Technology Accessibility, 36 C.F.R. §1194, issued under Section 508 of the Rehabilitation Act of 1973,

as amended (29 U.S.C. § 794(d)) (the "Section 508 Standards"), and (2) the Web Accessibility Standards, (the "ITD Standards") issued by the Commonwealth of Massachusetts' Information Technology Division ("ITD"), available online at www.mass.gov/itd. For purposes of this Agreement, contractor's obligations pertaining to these standards shall be limited to those subsections thereof that have been certified by ITD and the Massachusetts Office on Disability as objective and measurable. Such subsections shall be posted by ITD at www.mass.gov/itd. The Section 508 and ITD Standards may be modified from time to time, and is responsible for compliance with the most current version in effect on the date that contractor executes the contract.

GDIT will comply with the RFR specification.

8.24.1. AT/IT Adaptive List

Attachment D- AT/IT Adaptive List attached hereto sets forth a list of the specific assistive technology (AT) (including class, brand, and version) and specific desktop configuration against which the contractor's deliverables will be tested under this Agreement (the "AT IT Adaptive List").

GDIT will comply with the RFR specification.

8.24.2. Software Developed Under the Agreement

Prior to commencing any design work under this Agreement, contractor's Project Manager and design professionals shall meet with State 911 Department to review the Section 508 and ITD Standards, and the AT/IT Adaptive List, and to discuss their impact on the design process.

The contractor shall test every software deliverable delivered under this Agreement, including the custom code created to customize commercial off the shelf software (COTS) (collectively, "Software Deliverables"), and any updates, new releases, versions, upgrades, improvements, bug fixes, patches or other modifications to the software ("Enhancements") developed under this agreement, against Section 508 and ITD Standards, and for interoperability with the AT and IT environment listed in the AT/IT Environment list. At the time each such Software Deliverable or Enhancement is delivered to the State 911 Department, the contractor shall deliver to the State 911 Department and the ITD Accessibility Laboratory (the "ITD ATL") the results of such testing

In addition, the contractor shall cooperate with the ITD ATL, and any Accessibility Testing Contractor engaged by the ITD ATL, or by the State 911 Department under the supervision of the ITD ATL, in the performance of testing. The ITD ATL, any Accessibility Testing engaged by the ITD ATL, or by the State 911 Department under the supervision of the ITD ATL, shall test each Software Deliverable or Enhancement against the Section 508 and ITD Standards, and for interoperability with the AT and the IT environment described in the AT/IT Environment List. The ITD ATL shall certify such deliverables or Enhancements as compliant with the Section 508 and the ITD Standards and interoperable with the AT and environment described in the AT/IT Environment List.

The contractor shall be responsible for curing each instance in which its deliverables fail to comply with the Section 508 or ITD Standards. The contractor shall use its best efforts to cooperate with the State 911 Department, the ITD ATL, and any pertinent AT to correct any problems identified during such testing with the interoperability of the Software Deliverables or Enhancements with the AT and the IT environment specified in the AT/IT Environment List.

The contractor shall provide a credit against amounts due by the State 911 Department under this agreement for all testing, including repeat accessibility testing required with respect to Software Deliverables or Enhancements that fail initial testing with respect to the Section 508 or ITD Standards and are required by the ITD ATL to be retested in that regard. Such credits shall not exceed 5% of either (1) the total fixed price due the contractor under this Agreement, or (2) the total not-to-exceed amount of this Agreement if entered under a time and materials basis.

GDIT and our team do not have software development planned under this agreement.

8.24.3. COTS and ASP Software

The contractor shall conduct testing against the Section 508 and ITD Standards, and for interoperability with the AT and IT environment listed in the AT/IT Environment list, on all COTS referenced in the contractor's bid that must be acquired by the State 911 Department in order to implement the system to be delivered by the contractor under this Agreement, and all COTS (including for purposes of this section COTS configured by the contractor), or software to be provided by the contractor or its subcontractors in their capacity as application contractors (ASP).

delivered under this agreement, and any Enhancements thereto or new versions thereof, prior to its delivery to the State 911 Department (collectively, COTS and ASP Software). The contractor shall deliver to both the State 911 Department and the ITD ATL the results of such testing with each delivery of COTS or ASP Software.

The contractor need not conduct such tests for COTS and ASP Software for which accessibility testing has already been conducted and test results have already been provided to the ITD ATL. Instead, the contractor shall provide notice to the State 911 Department that such software has already been certified by the ITD ATL. The notice shall include the name of the software or Enhancement, and the date the software was so certified.

The ITD ATL, or any Accessibility Testing Contractor engaged by the ITD ATL, or by the State 911 Department under the supervision of the ITD ATL, shall test such software for accessibility against the Section 508 Standards and the ITD Standards, and for interoperability with the specific AT and the IT environment set forth in the AT/IT Environment List. The ITD ATL shall certify as accessible all software so tested that complies with the Section 508 Standards and the ITD Standards, and is interoperable with the AT and the environment specified in the AT/IT Environment List, and shall maintain a central web-based list of certified software for use by the Executive Department.

The contractor shall be responsible for curing each instance in which its deliverables fail to comply with the Section 508 and ITD Standards. The contractor shall use its best efforts to cooperate with the State 911 Department, the ITD ATL, and any pertinent AT to correct any problems identified during such testing with the interoperability of the Software Deliverables or Enhancements with the AT and the IT environment specified in the AT/IT Environment List.

The contractor shall provide a credit against amounts due by the State 911 Department under this agreement for all testing, including repeat accessibility testing required with respect to Software Deliverables or Enhancements that fail initial testing with respect to the Section 508, ITD Standards and are required by the ITD ATL to be retested in that regard. Such credits shall not exceed 5% of either the total fixed price due Contractor under this Agreement, or the total not-to-exceed amount of this Agreement if entered under a time and materials basis.

The contractor shall not deliver COTS or ASP software under this Agreement that fails to meet such standards unless it has documented (1) that it has performed due diligence in seeking accessible alternative COTS or ASP Software, offering equivalent features and functionality to the inaccessible COTS or ASP Software, for which the contractor is or can readily become a licensed distributor; and (2) the cost of developing substitute accessible software under this Agreement. (Such documentation need not include reference to any specific competing COTS or ASP Software and its level of accessibility). COTS or ASP Software delivered under this Agreement or under another contract with a state agency in connection with a system delivered under this Agreement that does not meet the Section 508 Standards or the ITD Standards shall be acceptable if either (1) the software contractor provides a roadmap for meeting such standards and interoperating with such AT or (2) the agency seeks and obtains a waiver from ITD that it would be an undue hardship on the agency to eschew use of such COTS or ASP Software.

GDIT will comply with the RFR specification.

Section 9 – BIDDER QUALIFICATIONS

The bidder shall clearly display an extensive knowledge of and experience with Next Generation 911 principles, practices, and standards. The bidder shall have extensive knowledge of and active involvement with public safety principles and practices. The bidder shall have knowledge of and experience with regionalized and consolidated PSAPs, emergency communications systems and practices, IP-based network architecture, principles, engineering services, and network security, and other applicable technical expertise related to a large scale Next Generation 911 project. The bidder shall have knowledge of and active involvement with Next Generation 911 standards development organizations and professional organizations, including without limitation, participation in NENA Next Generation 911 committees. The bidder shall have demonstrated awareness of and experience with integration of access to Next Generation 911 services for persons with disabilities.

Bidder's response shall include a profile of its operations, qualifications and the organization capabilities, including but not limited to the following:

GDIT will comply with the RFR specification.

General Dynamics Information Technology (GDIT) Unified Communications business unit, based in Needham, Massachusetts, is the proposed prime contractor and systems integrator for the MA NG9-1-1 Emergency Communication System. GDIT will program manage and lead the migration efforts to include integration, testing, and acceptance for the end-to-end NG9-1-1 solution for the Commonwealth. GDIT will also be providing the Network Operations Center (NOC), Security Operations Center (SOC), and Help Desk solutions in support of ongoing operations.

GDIT has assembled a "best in class" team for this project. We have closely worked with each of the team members not only in the development of our response to your RFR, but on previous projects. The GDIT team consists of Synergem, DSS, DDTi, Emergency CallWorks, Windstream, and key equipment providers – companies that are actively involved in the development of NENA standards and protocols. All of our teammates selected bring extensive experience with E9-1-1 services and products. The experience that each of team member brings is summarized in the following pages.

Committed Market Leader of Advanced Mission-Critical Communication Transitions

GDIT is a market leader in the implementation of advanced mission-critical communication infrastructure transformations. Since 1999, GDIT has Engineered, Furnished, Installed, and Tested (EFI&T) Enhanced 9-1-1 (E9-1-1) systems for the DoD at bases worldwide. Specifically, GDIT is one of the largest providers of E9-1-1 solutions to the federal government, with over 70 ongoing and currently completed E9-1-1 implementations at United States Air Force (USAF) bases around the world. As part of this USAF initiative, we started with the development of the system requirements, through the solution evaluation, recommendation, and implementation, to include a multiphase pilot system design to migrate to the NG9-1-1 environment.

GDIT is committed to delivering exceptional value to our customers, and we bring significant experience at the state and local levels across a wide array of communication technologies, including TDM-to-IP voice network modernization, virtualization, security, network operations, and call center implementation.

Active E9-1-1 Experience with Over 16 Years in Emergency Communications

GDIT's Unified Communications (UC) business unit is leading our design and execution for MA NG9-1-1, leveraging over 20 years of voice implementation, operations, and sustainment expertise. GDIT is an industry leader with over 16 years of experience in the area of emergency communications. Contracted for over 70 E9-1-1 systems in the role of a systems integrator, GDIT has a proven track record of sustained superior performance in providing on-time, reliable systems in this critical area.

GDIT's active E9-1-1 experience within the DoD includes: implementing/deploying E9-1-1 systems at military installations worldwide; assisting the government effort to implement GIS (mapping) for E9-1-1 calls; and integrating the Public Switched Telephone Network (PSTN) and the DoD's Defense Switched Network (DSN) emergency call capability, delivering the same level of caller information (ANI/ALI/GIS) for all call types. GDIT has used a variety of deployment models, including: multi-agency (Fire, Law Enforcement, EMS) and multi-site (distributed PSAPs in single or multiple geographic base scenarios). GDIT also ensures these systems are adequately secured based on our wide-ranging experience in network security and Information Assurance (IA).

Turn-Key Implementation of Large Scale Projects

GDIT also has extensive experience implementing large-scale telephony projects. GDIT is the prime contractor for the 10-year Federal Aviation Administration (FAA) Administrative Voice Enterprise Services (FAVES) contract, providing a comprehensive architecture, design, engineering, transition, and operational management for an IP-based national converged voice communications network. This project is a prime example of our capability to successfully provide the full range of planning, engineering, implementation, sustainment, and transition functions on a large project. This enterprise architecture provides enhanced telephony services to the FAA's nearly 50,000 employees located at over 800 government-owned and -leased facilities throughout the United States and in many nationally strategic locations worldwide.

FAVES is a business-critical rehabilitation of the FAA's highly distributed, geographically dispersed voice network that delivers advanced IP communications services, highly reduced communication cost, and vastly improved operations – all with improved capability, flexibility, reliability, and continuity. GDIT is transitioning the current legacy Private Branch Exchange (PBX) based environment to a modern infrastructure based on Voice over Internet Protocol (VoIP) and IP Telephony (IPT) technologies in order to provide a greater degree of flexibility and capability at significantly reduced operating costs. GDIT provides day-to-day agency operations that include providing the FAA with enhanced telephony services within, between, and outside FAA facilities.

GDIT is working with the stakeholders and leadership at each location to carefully plan, facilitate, and support the new VoIP capabilities. This includes preparing and conducting training and support documentation.

Experience with Proposed System Technology: NG9-1-1 and ESInet Systems

For the past five years, GDIT has been implementing many elements of the NG9-1-1 architecture into DoD and FAA networks. During the past two years, GDIT has focused on the development of NG9-1-1 systems. For 15+ years, GDIT has been building working relationships with, and

integrating products of, technology partners providing key components to NENA i3-compliant NG9-1-1 solutions. Currently, GDIT is providing a complete turn-key EFI&T solution to implement a NENA i3-compliant NG9-1-1 solution for Morgan County, Ohio. It includes a fully functioning ESInet, and all routing is done spatially, based on geographic coordinates. NENA i3 compliance has been achieved by adherence to standards where they exist, fortified by intelligent engineering to bridge gaps in the standards, and tempered by practical modifications that improve cost-effectiveness without diminishing overall compliance.

The solution has been designed to achieve 99.999% availability with two cores, diverse routes, and critical monitoring and maintenance. All functional elements were pre-tested in our NENA i3 Solutions Interoperability Lab, staged on site, and deployed in phases. The initial capacity of the systems will support up to ten counties and can be expanded to encompass all agencies in the State of Ohio.

Additionally, GDIT has a NG9-1-1 i3 Solutions Interoperability Lab in our Needham, MA location, providing a dedicated infrastructure for interoperability testing, regression testing, upgrade management, and troubleshooting. The lab is brand agnostic, allowing our customers and prospects to determine which component provider best suits their individual needs and providing a location where custom configurations may be deployed for the purpose of risk mitigation on our customer's behalf.

Figure 94 gives an overview of our transition working towards NG9-1-1 solutions as well as our entrenchment in the public safety community with examples of projects we have supported and are currently working.

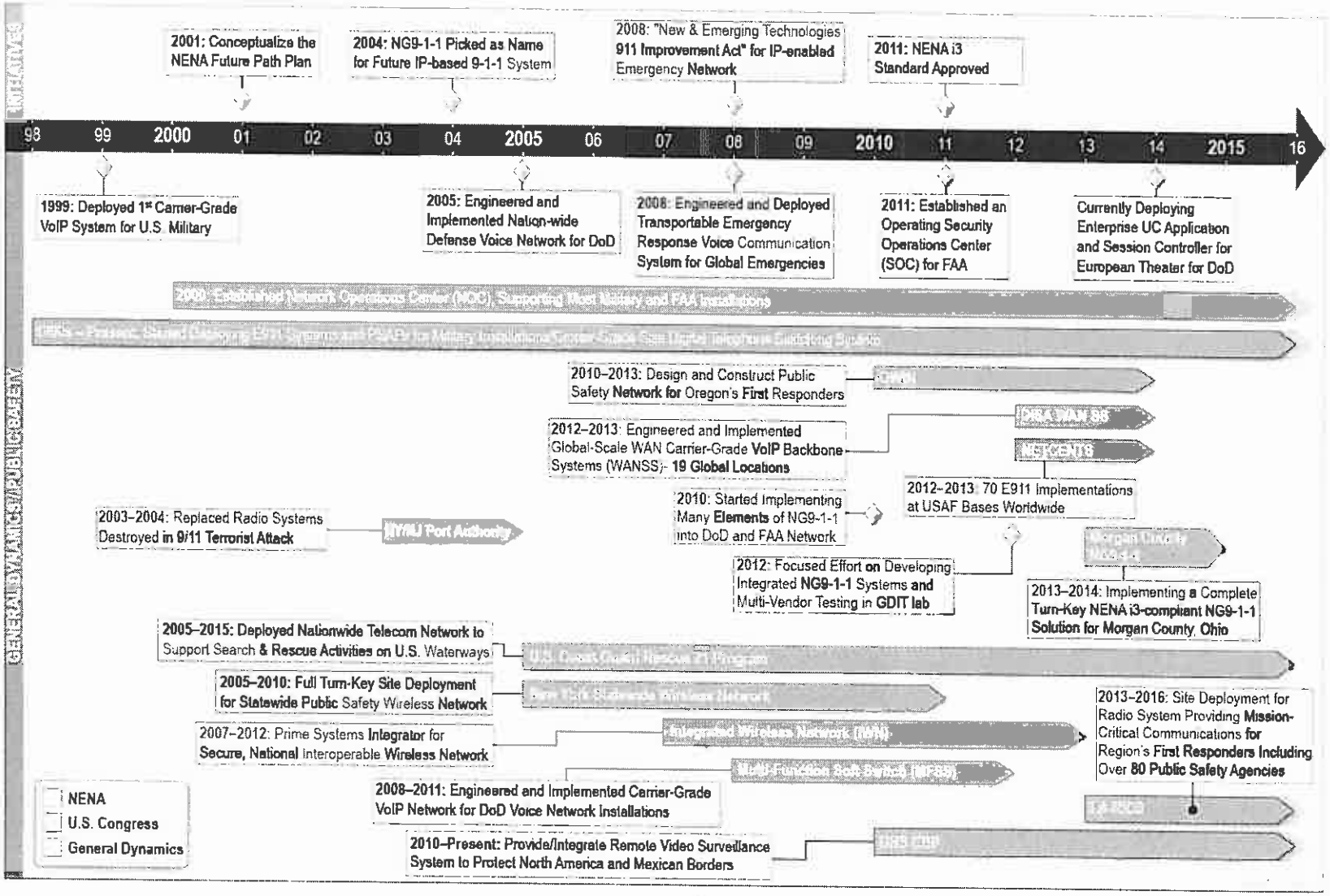


Figure 94. GDIT Transition Overview to NG9-1-1 Implementations

General Dynamics Corporation

An organizational chart;

The number of years the bidder has been in business and the number of years the bidder has been in the business identified in the RFR

General Dynamics, headquartered in Falls Church, VA, employs approximately 96,000 people worldwide generating $31.2 billion in revenue in 2013. The General Dynamics Corporation was officially established in February 21, 1952. The company is organized into four business groups: Information Systems and Technology (IS&T), Aerospace, Combat Systems, and Marine Systems, as shown in Figure 95. In 1999, General Dynamics acquired GTE Government Systems for $1.3B to strengthen its telecommunications and Information Technology (IT) capabilities and broaden its market reach. This acquisition formed the IS&T group made up of General Dynamics Command, Control, Communications, and Computing (GDC4S), General Dynamics Advanced Information Systems (GDAIS), and GDIT. GDIT is the business unit responding to the MA NG9-1-1 opportunity. GDIT Unified Communications has been providing E9-1-1, Land Mobile Radio (LMR), and other integrated telecommunications systems for mission-critical networks since 1999.

GDIT employs over 28,000 engineering, technical, and professional staff personnel in all 50 states delivering IT services and enterprise solutions serving federal, state, and local government customers.

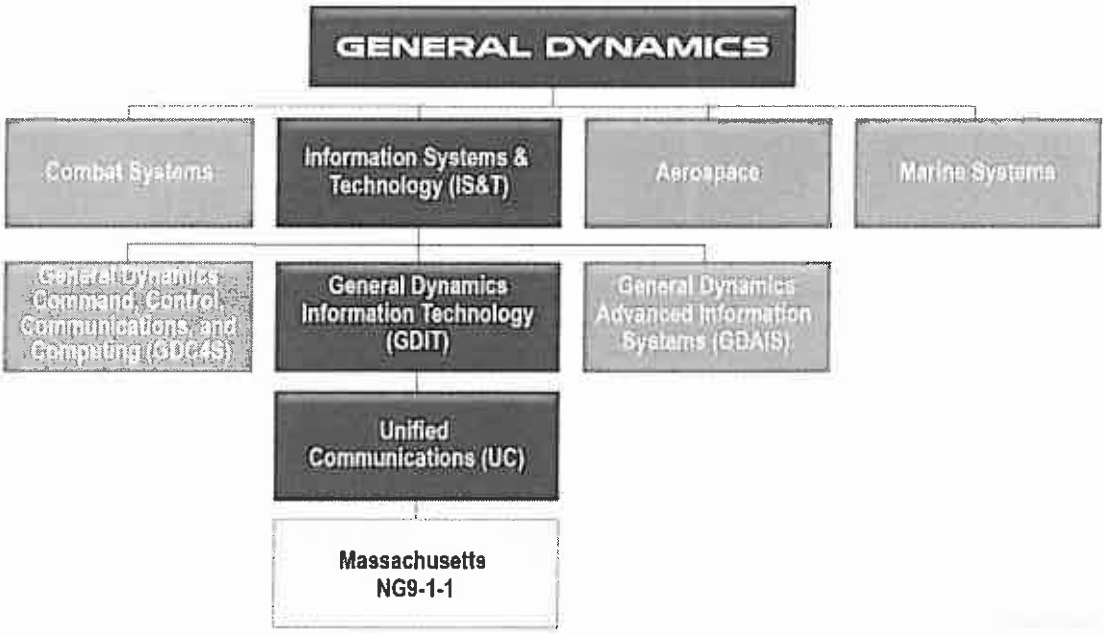


Figure 95. General Dynamics Organization Structure

Massachusetts-Based Employer

As a long time Massachusetts employer, GDIT has extensive working relationships with other Massachusetts business partners and a special commitment to the welfare and safety of the citizens of this state. Along with employing almost 3,200 people across Massachusetts, we

provide business to over 1,300 Massachusetts-based suppliers, as shown in Figure 96, totaling more than $490M in spending dollars over the past two years.

Congressional District	# of Suppliers	$ Spent
1	222	46,833,750
2	92	23,099,419
3	183	91,624,018
4	155	121,109,410
5	175	129,746,328
6	202	38,833,271
7	62	6,122,593
8	160	8,187,145
9	60	5,537,575
Undesignated	65	19,000,000
Total	1371	[illegible]

Figure 96. General Dynamics Massachusetts Supplier Investment 2012/13

The GDIT Team – Proven Experience

We have assembled a team of proven performers to provide the lowest risk solution to the Commonwealth. GDIT is currently teamed with some of our proposed strategic partners (DDTi, Oracle, and DSS) in providing a NENA i3-compliant NG9-1-1 production deployment for the State of Ohio project. Table 33 contains a summary of the GDIT team experience in large-scale projects of similar nature, multi-site 9-1-1 systems, and the proposed NG9-1-1 and ESInet systems technology. Table 34 lists our key equipment vendors.

Table 33. Highlights of GDIT Team Experience and Qualifications

Company	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems	Proposed System Technology: NG9-1-1 and ESInet Systems
GDIT	• 20 years of voice implementation, operations, and sustainment expertise • Over 70 E9-1-1 system implementations/deployments • Providing architecture, design, engineering, transition, and operational management for an IP-based national converged voice communications network for the FAA FAVES	• Providing turn-key EFI&T solution to implement NENA i3-compliant NG9-1-1 solution for Morgan County, Ohio • Deployed i3 Solutions Interoperability Lab • Designed multiphase system design pilot program to migrate USAF to the NG9-1-1 environment

Company	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems	Proposed System Technology: NG9-1-1 and ESInet Systems
	project	
Windstream	• MAGNet – 66 Site MPLS network providing State agencies with Commonwealth applications, e-mail, and Internet including diverse 200 Mb hub ports. Shared switch – diverse SIP trunks providing VoIP services to 26 Commonwealth agencies • 118-site MPLS network connecting courts in Massachusetts including diverse 200 Mb ports • 52-site MPLS network including a hub and disaster recovery failover routing for the Boston Housing Authority	• Activated over 500 high-capacity circuits for the United States Department of Defense (DoD) • Contracted with the Defense Information System Agency (DISA) to provide the Defense Enterprise Computing Center (DECC) with fiber infrastructure • Contracted with U.S. Army to provide network services, including voice, data, and secure Internet access services to Fort Detrick – serving 7,800 military, federal, and contractor employees with fault-tolerant communication solutions including highly reliable voice services utilizing multiple network access points to eliminate network-caused interruptions on more than 10,000 phone lines • Contracted to provide voice, data, and Internet services for the U.S. Department of Veterans Affairs in its Region 4 area, encompassing 11 states in the Northeastern United States
Emergency CallWorks	• 160 installed PSAPs across the U.S. with over 475 positions of call taking, mapping, and dispatch. • Multiple successful installations of hosted, networked 9-1-1 solutions • Certified by the State of Massachusetts for E9-1-1 call handling • Awarded Cuyahoga County, OH for Geo-Diverse Hosted and Managed 10-Year project covering 45 PSAPs and 140 positions	• Leader in Next Generation 9-1-1 Call Handling / Mapping technologies in legacy, networked and hosted models • Creator of the natively integrated call handling, mapping and dispatch integration into a single platform • Call Handling leader at the very first ICE event for VoIP based 9-1-1 • Active in NENA and Association of Public-Safety Communications Officials (APCO) organizations • Founding Member of Industry Council for Emergency Response Technologies (iCERT) • Presented at numerous State APCO/NENA conferences in 2013 as well as selected for several in 2014
DDTi	• Over 1,000 installations through reseller across the U.S. • Over 150 direct installations in PSAPs nationwide	• Active on various NENA committees writing NG9-1-1 standards and participated in several NENA Industry Collaboration Events: ICE3, ICE4, ICE5, and the most recent ICE8 event • Active participant in the Ohio ESInet committee and technical standards subcommittee • Presented at the 2013 Ohio NENA APCO conference regarding NG9-1-1 • Producer of high-quality GIS data sets (critical component of the NG9-1-1 solution) for 9-1-1 for over 10 years • Working on definition and development of ECRF/LVF for the last three (3) years • Live NG9-1-1 implementation in process
DSS	• Over 20 years working with state, local, federal, and DoD First Responder and Public Safety Environments Project Management	• Active on NG9-1-1 development and steering committees • Flagship communication logger, Equature, is

Company	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems	Proposed System Technology: NG9-1-1 and ESInet Systems
	• National installed base of over 1,000 PSAPs • 270 PSAPs for the Massachusetts State 911 Department • Multi-site Public Safety for Colorado State Patrol • 18 PSAP locations for West Central Texas Council of Governments	native NG9-1-1 platform • DSS Equature is designed to NG9-1-1 specifications, and it has been tested at every NENA ICE event to date • DSS CTO chairs NENA's ICE 8 (Recording and Logging) Planning Committee • MCC 7500 Integration has been fully tested in Motorola's lab
Synergem	• Extensive experience in all aspects of emergency communications included in deployment of NG9-1-1 systems • Staff participated in design and deployment of many national, mission-critical 9-1-1 systems for NASA and U.S. Department of Energy • Systems tested in numerous NENA ICE events	• Providing key, essential elements within ESInet. Proposed system technologies include NENA i3 ESRP and BCF as well as other NG9-1-1 functional elements such as LSRG, LNG, and LPG. • Routed the nation's first NENA i3 end-to-end call through ESInet • Four (4) years of experience with Evolution911 technology, the call-taking graphical user interface that brings NG9-1-1 capabilities to the dispatcher • Participated in numerous NG9-1-1 designs, proposals, and working groups – conversant with industry next generation trends, emerging technologies, and NENA i3 specifications

Table 34. Key Equipment Vendors

Company	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems	Proposed System Technology: NG9-1-1 and ESInet Systems
Oracle	• Acme Packet products have been delivering mission-critical multimedia applications for Public Safety communications networks for 12 years. • The Largest 1-1-2 and 9-1-1 providers use Oracle products, including deployments in alignment with NENA and 3GPP specifications – 92 of the top 100 carriers deploy Oracle's VoIP enabled solutions. • Handle emergency services traffic for the DoD, the largest enterprises and financial institutions in the country, as well as Internet 2 and most U.S. government agencies worldwide. • Products are globally deployed in IMS networks, which is the architecture to be used by FirstNet.	• Providing key components for implementation into NENA i3 compliant NG9-1-1 solution for Morgan County. • Deployed proposed components in NG9-1-1 interoperability lab in conjunction with GDIT. • Proposed components deployed in NG9-1-1 labs at Illinois Institute and Texas A&M, as well as FirstNet.
Cisco	• Industry leader in IP convergence systems including routing, switching, firewalls, voice PBX, and management systems.	• Supplier of key LAN/WAN network systems including switch and routing. • Key provider of data firewall and data security products including firewall, intrusion detection, and security management. • Providing hosted PBX with integration of survivable gateway between ESInet and PSTN for administrative calling.

Company	Large-Scale Projects of Similar Nature – Multi-Site 9-1-1 Systems	Proposed System Technology: NG9-1-1 and ESInet Systems
Aculab	• Aculab's GroomerII signalling and media gateway will provide critical integration between IP and SS7 networks. This seamless integration is a fundamental requirement for emergency services organizations that are looking to deploy IP-based technology.	• Aculab products have been used in numerous systems that have transitioned from legacy systems to IP-based technology.

Experience and Other Projects Relevant to the RFR Performance Requirements

A detailed description of the bidder's experience and other projects relevant to the RFR performance requirements set forth in this RFR, including a description, dollar value, and the duration of the relevant projects;

GDIT has included detailed descriptions of relevant projects in this section. Table 35 gives a brief summary of each project, and more detailed descriptions follow the table. Subcontractor experience is found in section titled "Summary of the Qualifications and Experience of Subcontractors."

Table 35. Summary of Relevant Projects

GDIT Project	Relevancy
Morgan County, Ohio NG9-1-1 Deployment	**Technology, Engineering and Project Management** – GDIT is the prime contractor for a turn-key i3 NENA compliant NG9-1-1 solution.
Federal Aviation Administration (FAA) Administrative Voice Enterprise Services (FAVES)	**Technology Engineering and Project Management** – GDIT is the prime contractor on 10-year program for enterprise migration from legacy environment to IP including life cycle management, security, and network operations, addressing all facets of the telecommunications network.
United States Coast Guard National Distress and Response System Modernization Project - Rescue 21	**Engineering and Project Management** – General Dynamics is the prime contractor and systems integrator for developing and deploying the USCG's primary maritime communications system for coastal C2. Rescue 21 is enhancing the USCG's ability to detect mayday calls, locate their source and coordinate rescues along the U.S. coastline, Great Lakes region, Hawaii, Guam, and San Juan. Work includes Rescue 21 installation on more than 230 remote sites.
E911 System at Elmendorf Air Force Base, AK	**Technology, Engineering and Project Management** – GDIT is the prime contractor to Engineer, Furnish, Install, Test, and Culover (EFIT&C) an integrated E911 system at and between Elmendorf Air Force Base and Fort Richardson, in Anchorage, Alaska.
E911 System at Ellsworth Air Force Base, SD	**Technology, Engineering and Project Management** – GDIT is the prime contractor to EFI&T a large E911 deployment including the integration of LMR, video displays, dispatch consoles, call routing, CAMA trunks, and network connections.
Defense Information Agency System Wide Area Network Soft Switches – DISA WANSS	Technology, **Engineering and Project Management** – GDIT is the prime contractor for a multi-phased modernization and migration of the Defense Information System Network (DISN) backbone for worldwide access and transport. Includes Acme Packet/Oracle Border Control Function. This network supports over one million DoD users and has maintained 99.999% reliability and availability.
East Orange Police Department (EOPD)	**Training** – One of multiple Jersey City Police Department (JCPD) projects where GDIT migrated the existing data from a JCPD legacy application, installed and configured the server applications, trained personnel, and established an independent training server for employees. GDIT provided the interface to and modification of E911 ANI/ALI to third-party controller, the integration of an Arrest system to Dynamic Images Mug Shot application, and the integration of CAD to Info-Cop – Gold Type Business Machines (GTBM), Inc.'s New Jersey State Interface and AVL application.
Long Beach Island (LBI)	**Training and Software** – One of multiple Jersey City Police Department

GDIT Project	Relevancy
	projects where GDIT migrated the existing data from a JCPD legacy application, installed and configured the server applications, trained personnel, and established an independent training server for employees.
Jersey City Police Department (JCPD)	**Training and Software** – One of multiple Jersey City Police Department projects where GDIT migrated the existing data from a JCPD legacy application, installed and configured the server applications, trained personnel, and established an independent training server for employees. GDIT provided the interface to and modification of E911 ANI/ALI to third-party controller, the integration of an Arrest system to Dynamic Images Mug Shot application, and the integration of CAD to Info-Cop – Gold Type Business Machines (GTBM), Inc.'s New Jersey State Interface and AVL application.
Department of State Antiterrorism DoS ATA Program Course Development Support	**Training** – GDIT developed and conducted training technical assistance courses for selected government law enforcement and security forces to enhance law enforcement organizations' capabilities to better predict, prevent, respond to, and mitigate the effects of terrorism.
DSS 0125 – Effective Communication in DoD Security	**Training** – GDIT conducted a collaborative approach to develop training for mid-career security officials.
Naval Education and Training Professional Development and Technology Center (NETPDTC) Training Products and Support (NTPS)	**Training** – GDIT provides training products and support services to DoD customers on the Naval Education and Training Professional Development and Technology Center contract. We have developed many Section 508–compliant web-based courses under the NETPDTC contract that currently reside on the Navy Knowledge Online (NKO) portal.

PROJECT NAME: MORGAN COUNTY, OHIO NG9-1-1 DEPLOYMENT
Value: $527,237
Duration: 8/2013–8/2015
Point of Contact: David L. Bailey, 911 Coordinator, 740-541-9110, Davidlbailey10@embarqmail.com

Description: General Dynamics is providing a NENA i3-compliant NG9-1-1 production deployment for the State of Ohio (by county) with a fully functioning ESInet with spatial routing, based on geographic coordinates. Our ongoing Ohio project is a complete NG9-1-1 construct with adherence to NENA standards, fortified by intelligent engineering to bridge gaps in the standards, and tempered by well-conceived implementation strategies to improve cost-effectiveness without diminishing overall compliance. The solution has been designed to achieve 99.999% availability with two cores, diverse routes, and critical monitoring and maintenance. All functional elements were pre-tested in our NENA i3 Interoperability Lab, staged on site, and deployed in phases. As with Massachusetts, strategic partners in Ohio include: DDTi, Oracle, and DSS. The initial capacity of the systems will support up to ten counties and can be expanded to encompass all agencies in the State of Ohio. The Ohio project is expected to go live in June 2014

PROJECT NAME: FAVES
Value: $228M
Duration: 11/2009–10/2019 (5-year base and five 1-year options)
Point of Contact: Gloria Richmond, Technical Representative/COR, 202-267-7340, gloria.richmond@faa.gov

Description: GDIT is the prime contractor for the 10-year Federal Aviation Administration (FAA) Administrative Voice Enterprise Services (FAVES) contract, providing a comprehensive architecture, design, engineering, transition, and operational management for an Internet Protocol (IP) based national converged voice communications network. This enterprise architecture provides enhanced telephony services to the FAA's nearly 50,000 employees located at government-owned and leased facilities throughout the United States and in many nationally strategic locations worldwide.

FAVES is a business-critical rehabilitation of the FAA's highly distributed, geographically dispersed voice network that delivers advanced IP communications services, highly reduced communication cost, and vastly improved operations – all with improved capability, flexibility, reliability, and continuity. GDIT is transitioning the current legacy Private Branch Exchange (PBX) based environment to a modern infrastructure based on Voice over Internet Protocol (VoIP) and IP Telephony (IPT) technologies in order to provide a greater degree of flexibility and capability at significantly reduced operating costs. We provide day-to-day agency operations that include providing the FAA enhanced telephony services within, between, and outside FAA facilities.

GDIT is providing the full range of planning, engineering, implementation, sustainment, and transition functions to the FAA for this program. We are working with the stakeholders and leadership at each location to carefully plan, facilitate, and support the new VoIP capabilities. This includes preparing and conducting training and support documentation.

The established enterprise architecture supports the FAA's vision for enabling an FAA-wide administrative voice enterprise for the delivery, management, and operation of telephony services. GDIT modifies and develops enhancements for the existing PBXs to ensure continued supportability and/or enhance interoperability of these existing systems toward the enterprise architecture. Functional elements include:

- **Telephony Hosting Service** – provides consolidated and centralized voice applications and services such as voice mail, Automatic Call Distribution (ACD), Interactive Voice Response (IVR), and reservation-less voice conferencing. The telephony hosting service is based on an IP-Multimedia Subsystem (IMS) framework architecture that allows future applications to be added to all FAVES subscribers from a centralized location.
- **Public Switched Telephone Network (PSTN) Gateway Service** – provides Time-Division Multiplexing (TDM) and Session Initiation Protocol (SIP) trunk interfaces and allows connectivity to outside networks, such as the Federal Telecommunications System (FTS) or Networx. Continuity of operations is provided by a fully survivable capability for reaching the PSTN when the IP Wide Area Network (WAN) is lost.
- **IP-Enabling Service** – allows legacy PBXs to route through the IP WAN.

- **User Station Service** – legacy user stations and telephones are supported regardless of make, model, or manufacturer; user stations have access to telephony hosting service in the core system.
- **Special (DSN/FTS) Gateway Service** – leverages the FAA's existing Class 4/5 capable switches in Washington, D.C., and Oklahoma City. We provided interfaces to these existing switches that are Joint Interoperability Test Command (JITC) certified for Defense Switched Network (DSN) tandeming (multifunction switch). Additionally, JITC-certified solutions were fielded at the FAA's Command Center to provide services for both FAA and Air Force occupants. These highly scalable, flexible gateways are interoperable with PSTN, FTS, Networx, General Services Administration (GSA), and internal FAVES networks. These special gateways support continuity of operations through fully survivable failover for the IP WAN connectivity. The flexibility and interoperability includes the ability to provide Signaling System 7 (SS7) for access to public advanced intelligent network or intelligent network features.
- **Legacy User Stations** – GDIT's architecture allows legacy phones to be carried over the government-provided IP WAN when integrated. In addition, enterprise feature sets can be provided to those legacy users.

Transition: FAVES has created a national transition process and capability to support technical refresh and transitioned 350+ sites in less than four years. To date, GDIT has implemented the centralized voice service delivery core sites and has transitioned approximately 20% of the FAA user base and over 40 remote sites with enterprise VoIP, voice mail, and voice conferencing capabilities. FAVES is supporting multiple vendor VoIP platforms (e.g., Cisco, Avaya, Nortel, Alcatel), but we have designed a single enterprise core architecture to support all the platforms.

Program Management: The building blocks of the GDIT team's FAVES integrated management approach provide the structure needed for efficient program execution, management insight into program status, and quick resolution of potential problems. These critical components include: Contract Work Breakdown Structure, Integrated Master Plan, Integrated Master Schedule, Performance Measures, Program Organization Structure, Risk Management Plan, and Subcontract Management Plan.

Mutual success on the FAVES program is attributable to effective organizations, dedication to mission support, open lines of communication, and accountability. GDIT provides a proven Enterprise Program Management approach governing personnel and resources to deliver efficient operations, maintenance, management, administrative, logistics support, training support, and technical support to meet or exceed FAVES performance requirements. Our approach adheres to our ISO 9001:2008 Quality Management System (QMS) principles, processes, and procedures that are consistent, repeatable, and continually improved and applied with demonstrated success. We apply our QMS consistently, building on other relevant programs and lessons learned that provide the foundation for our enterprise program management approach. We have defined Key Performance Indicators (KPIs) that will enable the program team to monitor and predict program performance. The KPIs are reviewed by the Integrated Product Teams (IPTs) weekly and by the Program Management staff and key staff management personnel at least monthly. The KPIs are based on the information needed to monitor the health of the program.

Every successful program includes a Program Management Plan (PMP). The PMP provides a playbook for the team and the customer that is used for all aspects of program and contract performance. We use one set of tools, policies, and procedures – including well-defined communication and interaction plans – to assure same-page execution from contract day one to contract closeout. We provide our PMP to the FAA for review and approval to ensure we operate under a common framework toward achieving FAVES performance and cost objectives.

GDIT employs the Common Process Framework (CPF) on FAVES, an integrated set of web-based tools, procedures, templates, and checklists that provides the methodology and guidelines used to perform for the program. The CPF implements an efficient way to take the universe of methodologies – management, technical, external, and internal – and puts them into a common framework at a single site for team members and other stakeholders to guide consistent program execution.

Test and Acceptance: To date, GDIT has installed, tested, verified, and validated the migration through a series of exacting test and acceptance procedures for over 30 sites that are being converted from legacy systems to the FAA enterprise. Site migrations include the integration of the passive and active equipment constituting the FAVES infrastructure as well as verification and assessment of the Government-Furnished Equipment (GFE) services (Wide Area Network (WAN), Local Area Network (LAN), etc.).

GDIT provides all the labor, test equipment, and tools required to perform government-witnessed acceptance testing of each facility migration including the integration of any affected GFE and Government-Furnished Material (GFM); government acceptance also includes specific contract CLINs as required by the FAA that could include a complete set of engineering design documents, installation drawings, system test and acceptance reports, site-specific implementation plan, and manuals.

Operations: GDIT provides comprehensive operational services for over 360 voice switching systems nationwide. The GDIT–provided services support both legacy and transition networks. Through the employment of both GDIT and subcontracted resources, we provide services that include but are not limited to: transitioning, operating, system administration, maintaining, restoring, protecting, and performing backups of voice switching systems. GDIT also provides administrative-type support such as configuration management, asset management (hardware and software), and properly disposing of all voice switching systems and data. In addition to providing normal operations to the FAVES supported voice systems, GDIT provides 24x7x365 security operations. This includes monitoring all FAVES assets from a security perspective and reporting issues with the appropriate FAA internal security organizations and coordinating fix actions. This support includes meeting FAA Certification and Accreditation (C&A) standards.

Operational support covers all backroom and core hardware, including telephones and servers; software (operating and application); network operations and monitoring; and networking and transport solutions, including but not limited to: switched networks and non-standard technologies; distribution systems; switched and non-switched services; fiber optics; teleworking capabilities; and contingency operations and exercises.

Maintenance: GDIT's maintenance program supports the entire life cycle of the systems supported by FAVES. This includes legacy stand-alone solutions as well as enterprise-connected

solutions. In 2012, GDIT responded to over 10,000 different incidents ranging from Moves, Adds, and Changes (MACs) to trouble calls, preventative maintenance inspections, and material-related actions.

For Tier I maintenance, GDIT relies on on-site resources to immediately respond to customer service requests and/or outage situations, while less-critical locations are supported by GDIT's vast network of service providers to respond within the required Service-Level Agreement (SLA). GDIT provides Service Desk Tier II/Tier III support from our Emergency Operations Command Center (EOCC) located in Fairview Heights, IL. All activities are tracked and managed by the Service Desk to provide a central location for all reporting via GDIT's Remedy Incident Management System.

Sustainment: GDIT performs sustainment activities through operational hardware and software upgrades to improve network system reliability and availability. Through a robust Configuration Control Board (CCB) process, GDIT conducts full system-level testing, including integration and regression testing, to identify and resolve issues prior to releasing to the operational network. Engineering implementation packages are developed for software upgrades in order to facilitate software update deployment across active devices.

Quality of Service: GDIT continues to provide a long-standing history of high-quality service to the FAA as evidenced by our recurring excellent customer satisfaction surveys. Through an aggressive program that stresses proactive monitoring, timely reporting, and expedient responses to situations, GDIT ensures uptime of voice switching systems that borders on 99.99% for legacy systems, with enterprise systems consistently maintaining 99.999% or better.

Additionally, GDIT ensures constant feedback through a variety of scheduled as well as informal meetings with FAA leadership to include the Program Manager, Contracts Manager, and various Telecommunications Network Operations Managers (TNOMs). Weekly updates, bi-weekly in-person status briefings, and monthly program status reports all contribute to keeping the focus on quality service through exceptional performance – performance that is continually evaluated using quantifiable measurements provided by our numerous management and tracking systems.

Configuration Management: GDIT ensures fully compliant configuration control through the use of procedural and automated Configuration Management (CM) processes to control the process as requirements flow through various internal (GDIT) and external (Government) Configuration Control Boards (CCBs); these processes ensure design integrity and product baseline control. GDIT uses a Virtual Program Office (VPO) to maintain configuration control and version control of all design information.

Training: GDIT provides on-site training for the FAA users during the cutover/transition period. By employing a "train the trainer" approach, GDIT ensures local personnel receive the necessary training to address and support operational issues at the local level while ensuring all personnel have the requisite knowledge and information needed to effectively and efficiently use their new VoIP system. GDIT provides "leave behind" materials such as product information, training documents, and a customer service guide to reinforce and bolster the classroom training. The majority of the documentation is also hosted on an FAA internal website to ensure that end users have easy access to this information. GDIT coordinates with the FAA for all changes in the documentation prior to release.

Delivery Schedule: GDIT successfully manages all aspects of the integrated master schedule through a combination of internal and customer-directed review meetings and processes. Weekly updates are provided to the program office and these are augmented by project-specific interchange/status meetings and monthly reports. To date, GDIT has successfully met all program-directed milestones for both program-level and project-level initiatives. Our team has established processes for successfully meeting these deliverable dates and keeping the overall project on schedule.

Use and Control of Subcontractors: GDIT partners with a multitude of small and large businesses to provide support across the country, with the majority of the support provided across approximately 10 different partners. In total, GDIT has processed more than 400 requests for FAA personnel badges to support the FAVES contract, with 65% of the personnel badges issued to subcontractors. By effectively managing these local subcontractors, GDIT is able to minimize costs to our customers while meeting or exceeding customer expectations. More than 40% of all the business that was subcontracted is completed by or purchased through small businesses.

Controlling Project Cost: GDIT effectively controls project costs through a rigorous engineering/proposal development/implementation process that is monitored by our Defense Contract Audit Agency (DCAA) approved cost accounting system. Stringent guidelines for product selection are coupled with aggressive cost proposal reviews, ensuring all project costs are contained prior to submitting a price proposal to the FAA. Upon award of a task/delivery order, GDIT re-engages with Original Equipment Manufacturers (OEMs), providers, and subcontractors to ensure original costs were maintained; this process guarantees GDIT's Firm-Fixed Price proposals are free from the risk of uncontrolled or unwarranted cost increases.

In addition to controlling the FAVES costs, GDIT has been very active in supporting the FAA's initiatives to lower overall costs to the agency. Through extensive Return on Investment (ROI) analysis, our team works closely with the various organizations within the FAA to identify areas where costs savings can be obtained and plan migrations accordingly. Under this advisement, the FAA is on target to reduce spending in some areas (service contracts, circuits, long distance, etc.) by millions of dollars annually compared to the previous legacy environment. While those cost benefits alone may not seem dramatic, it should be noted that those savings are realized while upgrading/improving a significant portion of the administrative telecommunications infrastructure. So, not only is this a cost benefit, but it is avoiding legacy upgrade and replacement costs while providing significantly more features and functionality to the end users.

PROJECT NAME: UNITED STATES COAST GUARD RESCUE 21 PROGRAM
Value: (Inception to Date) $110M
Duration: 9/2002–9/2015
Point of Contact: Gene Lockhart, Rescue 21 Deputy Program Manager, 202-475-3144, eugene.g.lockhart@uscg.mil

Description: General Dynamics is the prime contractor for the USCG National Distress and Response System Modernization Project (NDRSMP) Phase II (Rescue 21) contract. The program involves the design and development of the system, site design, and implementation of all communication towers, and installation of all shore-based equipment at USCG Stations and

Sector Command Centers. It includes upgrades of shore facilities, development of Disaster Recovery Assets to support recovery from man-made and natural disasters, operational field maintenance, software maintenance, patch deployments, continuous network monitoring and fault detection, and 24x7 on-call user support. General Dynamics' O&M services support a suite of radio towers deployed in more than 240 locations over an area covering more than 300,000 square miles.

Since the initiation of Full Rate Production, we have conducted 32 Regional System Acceptance Tests 100% on time or early, at or below cost targets established by the customer.

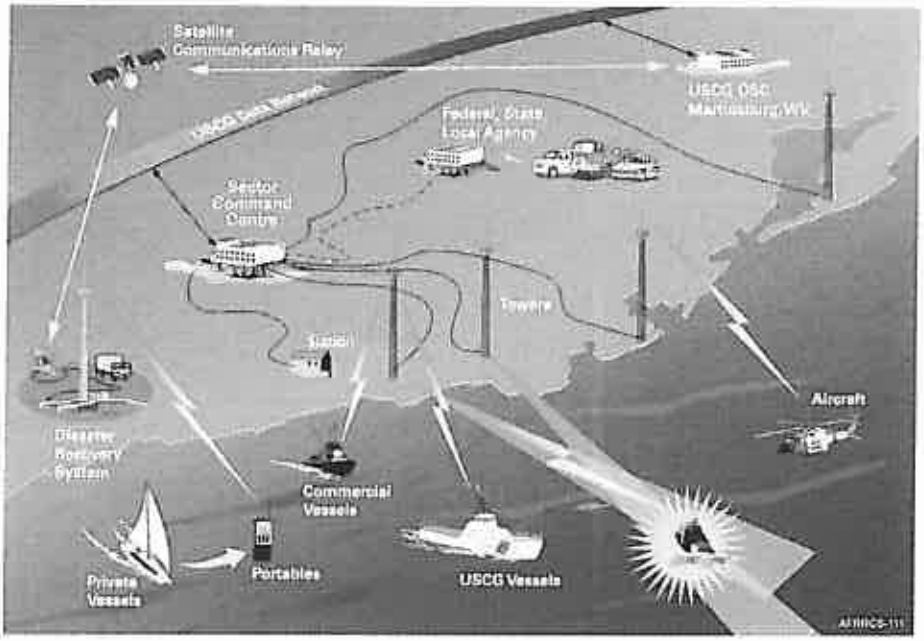


Figure 97. Rescue 21 Program Topology

The Rescue 21 program replaces an outdated National Distress Response System (deployed in 1970) with a leading edge VHF/UHF communications system covering coastline, navigable rivers, and waterways in the continental United States, Hawaii, Guam, and Puerto Rico. The Rescue 21 program's objective is to provide the USCG enhanced communications to save lives at sea and protect our nation's coastline.

Rescue 21 provides an updated, leading-edge communications system. By harnessing direction finding and/or global positioning and cutting-edge communications technology, Rescue 21 enables the Coast Guard to perform all its missions with greater agility and efficiency. The new system will close 88 known coverage gaps in coastal areas of the United States, enhancing the safety of life at sea. The expanded system's frequency capacity enables greater coordination with the Department of Homeland Security (DHS), other federal, state, and local agencies, and first responders.

Rescue 21 revolutionizes how the USCG uses command, control, and communications for all missions within the coastal zone. The system incorporates direction-finding equipment to improve locating distressed mariners, improve interoperability amongst federal, state, and local

agencies, reduce coverage gaps for coastal communication in and along navigable rivers/waterways, and provide the following system enhancements:

- Clarity of distress calls
- Allows simultaneous channel monitoring
- Upgrades the playback and recording feature of distress calls
- Supports digital selective calling for registered users
- Provides portable towers for restoration of communications during emergencies or natural disasters in the contiguous 48 states

General Dynamics' services include replacing and modifying a wide range of aging, obsolete radio communications equipment to include consoles at USCG Sectors and Stations and all remote transceiver sites (antenna towers), as well as the network connecting them to the appropriate sector. We recognize the crucial need to meet schedule requirements for key public safety networks like Rescue 21. We know that lives depend upon a public safety network. The Rescue 21 network has supported over 30,000 Search and Rescue cases.

PROJECT NAME: E911 SYSTEM AT ELMENDORF AIR FORCE BASE, AK
Value: $1M
Duration: 11/2011–9/2012
Point of Contact: Steve Ryder, Site POC, Telephone Maintenance Technician, (907) 552-9700, steven.ryder.2@us.af.mil

Description: GDIT provided a complete JITC- certified upgrade to the current E911 system at Elmendorf Air Force Base, Alaska that included the installation of seven (7) Graphical User Interface (GUI) based E911 operator dispatch console positions; each console was equipped with two (2) separate monitors (one for telephony and the other for LMR operation). GDIT's solution was based on the Cassidian VESTA system and included key features and benefits such as being JITC-certified for both Interoperability and IA, automatic TTY detection, and full TTY response capability, integration to GFE NICE voice recorders, overflow routing, emergency ringback, and on-site training. The VESTA E911 system interfaces directly with the existing Joint Base Elmendorf-Richardson (JBER) telephone switches and CAIRS telephone management system. The GDIT solution integrates with the CAIRS database to provide the ability to receive and process all ALI/ANI information from all JBER switches necessary to ensure emergency response to residential, cellular, and official 911 calls originating from the greater JBER complex.

GDIT's solution provides seven (7) VESTA APs consisting of a computer workstation equipped with two (2) 20-inch flat panel touchscreen monitors, a mouse, keyboard, 24-button Genovation keypad, and ACU. One monitor displays the VESTA application and the second monitor displays the LMR/Alaska Land Mobile Radio (ALMR) system. The VESTA and radio console workstations share the keyboard and mouse via the government-provided KVM. The Elmendorf AFB implementation includes audio integration with the GFE LMR/ALMR radio console, providing a common headset/handset. The radio console provides arbitration in the event of simultaneous traffic, passing the radio audio to external General Purpose I/O Module (GPIOM) connected speakers, and retaining the telephone audio in the user's headset or handset.

PROJECT NAME: E911 SYSTEM AT ELLSWORTH AIR FORCE BASE, SD
Value: $1.03M
Duration: 6/2009–7/2010
Point of Contact: Wendy Farley, 84 CBSG PK, 6029 Wardleigh Rd., Bldg. 1207, Hill AFB, UT 84056-5838, (801)-586-3464

Description: GDIT provided a turn-key EFI&T solution to implement a JITC-certified and Approved Products List (APL) compliant E911 system at Ellsworth Air Force Base in South Dakota. The new computer-based Cassidian VESTA M1 system includes being JITC-certified for both Interoperability (IO) and Information Assurance (IA), and includes comprehensive telecom integration, extensive system and user configurations, 24-inch LCD monitors, automatic TTY detection and full TTY response capability, integration to GFE NICE voice recorders, integration with the existing Motorola LMR system, and on-site training.

The system supports E911 calls from the base S8700 Host switch, the Financial Services Avaya S8500 switch, and the base lodging Avaya G3Si, and supports hot flash or start code transfer to Security Forces or the local Pennington County E911 center. GDIT's E911 solution provides TDD/TTY capabilities and includes training one instructor for the Fire and Security Forces units on TDD/TTY. The GDIT solution includes four (4) VESTA Answering Positions (APs). Each of the four (4) PSAPs communicates over the existing Ellsworth AFB network infrastructure to provide immediate redundancy in the event of a failure at the primary location.

The E911 system is designed to report full Caller Identification information for on-base prefixes (base housing, mercantile facilities, BX, Commissary, Shoppette, and base payphones) and exchanges to include calling number, name, and location (ANI/ALI), and will overcome Caller ID blocking. Calls answered on lines designated in the VESTA system as emergency lines utilize the received 10 digit Calling Line ID (CLID), Calling Party Number (CPN), or ANI to collect location information from the appropriate ALI source. VESTA identifies the appropriate ALI source based on Directory Number (DN) assignment, sending the ALI request to either the PEAbody system for PBX extension–originated emergency calls or to the public ALI provider for Public Switched Telephone Network (PSTN) originated E911 calls. The VESTA console consists of a computer workstation equipped with two (2) 24-inch flat panel screen monitors, a mouse, keyboard, 24-button Genovation keypad, and Audio Control Unit (ACU). One of the monitors displays the VESTA application and the second monitor replaces the existing display on the GFE LMR system. The VESTA and radio console workstations share the keyboard and mouse via the government-provided Keyboard, Video, Mouse (KVM).

The Ellsworth AFB implementation includes audio integration with the LMR radio console, providing a common headset/handset. The radio console provides arbitration in the event of simultaneous traffic, passing the radio audio to external General Purpose I/O Module (GPIOM) connected speakers, and retaining the telephone audio in the user's headset or handset. In addition, our solution provides features so all calls can be placed on hold and connected to another console via the "Conference" feature, or transferred to another party such as the Security Forces Squadron Law Enforcement Desk (LED).

This contract was completed on budget.

PROJECT NAME: DISA WANSS
Value: $13M
Duration: 2012–2013
Point of Contact: Marc Crandell, Program Manager, Hill AFB, UT, (801) 586-5559
Marlon Mailey, Program Manager, HQ DISA, Fort Meade, MD, (301) 225-2491

Description: GDIT has implemented all Defense Information Agency System (DISA) Unified Communications (UC) systems, including 19 Wide Area Network (WAN) soft switches globally and several of the voice, video, and data implementations for the USAF. GDIT has Engineered, Furnished, Installed, and Tested (EFI&T) integration of Defense Connect Online (DCO) conferencing capability as well as all six (6) Voice Internet Service Provider (V-ISP) gateways. GDIT is uniquely qualified to provide both Time-Division Multiplexing (TDM) and IP-based voice systems, to include E911 systems and NG911 systems. Within the last two years, our Unified Communications team implemented over 70 E911 systems. GDIT's roles and areas of expertise include: prime contractor and lead systems integrator; system engineering; program management (PMP certified project leads); Network Operations Center (NOC) support; installation, surveillance, and support; UC engineering experience; and system integration of UC infrastructure. Key personnel include a program manager, system engineers, and a solutions architect.

The DISA UC in support of Department of Defense (DoD) Military Departments (MILDEP) provides network infrastructure as specified in the DoD Unified Capability Requirements (UCR). General Dynamics, in support of DISA, engineered and provided the Wide Area Network Soft Switches (WANSS), which consists of Engineer, Furnish, Install, and Test (EFI&T) at multiple locations throughout the world providing converged Voice and Video over IP (VVoIP) and Unified Communications (UC) capability across the Defense Information Systems Network (DISN) backbone. Our responsibilities included providing all task order administration, task order management, personnel, tools, equipment, material, consumable supplies, and services associated to Engineer, Furnish, Install, and Test (EFI&T) WANSS to include Soft Switches, Session Border Controllers (SBC), Media Gateways (MGs), Network Timing source, Customer Edge routers, network security and intrusion protection systems, Network Storage, and any other associated ancillary equipment necessary for the highly reliable carrier-grade enterprise network. The systems we provide had to meet and be certified for strict DoD specifications and information security requirements.

These WANSS projects required subject matter expertise in all ranges of telecommunication systems skills to include TDM and IP-based voice systems, data network engineering, IP information security, session border controllers, intrusion protection, and data storage.

PROJECT NAME: EAST ORANGE POLICE DEPARTMENT (EOPD)
Value: $343,969
Duration: 2005–2013
Point of Contact: Chief William Robinson, East Orange Police Dept, NJ, (973) 672-4549

Description: EOPD required the replacement of an existing client-server Computer Aided Dispatch/Records Management System (CAD/RMS) application with GDIT's Law Enforcement Advanced Applications (LEAA) system; modification of ANI/ALI to third party controller;

integration of an Arrest System to the Dynamic Images Mug Shot application; and integration of CAD to Info-Cop – Gold Type Business Machines (GTBM), Inc.'s New Jersey State Interface and AVL application.

Technical Approach: GDIT migrated the existing data from a JCPD legacy application, installed and configured the server applications, trained personnel, and established an independent training server for employees. EOPD required modifications of the LEAA application for successful operation within its infrastructure. EOPD also required systems that were not in the JCPD package, including:

- Increased the multi-level approval process in the RMS from two to three levels
- Added nine reports to the RMS system specific to EOPD needs
- Created a Mapping solution for crime analysis using MapInfo
- CAD interface to an AVL (third-party vendor) System
- Integrated a Mug Shot database application by Dynamic Images into LEAA
- Interfaced 911 ANI/ALI software to a third-party ANI/ALI provider
- Created a seamless interface between LEAA CAD and Info-Cop (State CJIS Interface) in mobile units
- CAD Silent Dispatch: Mobile CAD

EOPD contracted for the LEAA system with the additional systems listed above. GDIT customized the LEAA Core System and provided the additional systems as required. We also replaced an existing client-server CAD/RMS application with LEAA and modified ANI/ALI to a third-party controller.

GDIT also integrated the Arrest System to the Dynamic Images Mug Shot application. We integrated CAD to Info-Cop – GTBM's New Jersey State Interface and AVL application.

Benefits to EOPD included:

- Reduced hardware cost
- Reduced application downtime
- Reduce departmental overhead cost
- Greatly reduced learning curve and operational transition
- Real-time data analysis/statistics for police department management
- Expedient methods to deploy changes by departmental request
- Applied software upgrades without downtime

PROJECT NAME: LONG BEACH ISLAND (LBI)
Value: $144,790
Duration: 2007–2014
Point of Contact: Michelle DeGeso, Chief of Communications, (609) 494-3322

Description: In 2007, LBI contacted JCPD about its new GDIT Law Enforcement Advanced Applications (LEAA) system operations. They had the same legacy system as JCPD and were in constant contact with JCPD's IT divisions concerning ongoing problems. They were also aware of Beach Haven, which had been operating the GDIT VB System for over 10 years. A mutual agreement was reached to consolidate police software operations for the entire island. The original intent was to have a consolidated CAD System at LBI with dispatchers from Beach Haven relocated to LBI. It would be more cost-effective to the various towns to operate a central CAD dispatch system.

Beach Haven would retain its current in-house RMS system and hardware. Eventually, it was determined to have one RMS software solution rather than two. GDIT was required to make software modifications to protect police data for each agency. Only certain data is shared in the regional system.

LBI took the JCPD LEAA System "Off the Shelf" because they had the same legacy system as JCPD. However, LBI did require modifications in CAD for multi-agency dispatch and also requested additional modules that JCPD did not require. GDIT built the first multi-agency CAD/RMS System under the guidance of LBI and Beach Haven.

Technical Approach: GDIT migrated the existing data from a JCPD legacy application, installed and configured the server applications, trained personnel, and established an independent training server for employees.

Benefits to LBI include:

- Reduced hardware cost
- Reduced application downtime
- Reduced departmental overhead cost
- Greatly reduced learning curve and operational transition
- Real-time data analysis/statistics for police department management
- Expedient methods to deploy changes by departmental request
- Applied software upgrades without downtime
- Instrumental in process improvements, job task reallocation, job performance support tools, and training

PROJECT NAME: JERSEY CITY POLICE DEPARTMENT (JCPD)
Value: $1,839,627
Duration: 2004–2013
Point of Contact: John Tkaczyk, Sr. Systems Administrator, Jersey City Police Department, (201) 547-5997

Description: JCPD contracted GDIT to build a CAD/RMS System prototype based on the JCPD design and functionality. Since GDIT had been involved in the original character-based CAD /

RMS system, we understood JCPD's goals. GDIT built the prototype according to JCPD specifications and demonstrated it to the JCPD CAD / RMS committee, and a Purchase Order (PO) was executed to GDIT to develop a full-blown CAD / RMS package, our Law Enforcement Advanced Applications (LEAA) system. At that time, web-based solutions, although in infancy, were becoming cutting-edge technology. JCPD modified the contract and with additional resources determined the long-term benefit was to switch from a client-based CAD / RMS solution to a web-based solution. JCPD chose the GDIT client-based VB System as its base model.

JCPD created a task force called Police Automated Radio Records Information System (PARRIS) comprised of personnel from all divisions of JCPD. Its objectives were to design a new CAD / RMS System. The Task Force analyzed the department's Operations Infrastructure to determine data flow, functionality, and design of each system and module. PARRIS selected single data elements, location on the screen, data flow, and drop-down table requirements. PARRIS took almost 18 months to create the blueprints for CAD/RMS. Programming commenced as each major system was defined. During that time, JCPD operated its Legacy System. From a simple CAD ticket to a complex Bureau of Criminal Identification (BCI) Arrest / Booking Report, the team covered every field, every drop-down, and every requirement, as well as all security requirements for the system from Divisions to Units to Individual Logons.

Technical Approach: GDIT migrated the existing data from a JCPD legacy application, installed and configured the server applications, trained personnel, and established an independent training server for employees.

Benefits to JCPD include:

- Web-based system saved JCPD internal overhead costs in manpower and ongoing user support
- Reduced hardware cost
- Reduced application downtime
- Reduced departmental overhead cost
- Greatly reduced learning curve and operational transition
- Real-time data analysis/statistics for police department management
- Expedient methods to deploy changes by departmental request
- Applied software upgrades without downtime

Instrumental in process improvements, job task reallocation, job performance support tools, and training.

PROJECT NAME: DOS ATA PROGRAM – COURSE DEVELOPMENT SUPPORT
Value: $4.8M
Duration: 2006–2012
Point of Contact: Dottie McCubbin, Operations Coordinator, U.S. Department of State (DoS) Bureau of Diplomatic Security Office of Antiterrorism Assistance (ATA), (571) 226-9710

Description: ATA is responsible for providing training and technical assistance to enhance the capabilities of selected foreign governments' law enforcement and security forces. Training and assistance is designed to enhance law enforcement organizations' capabilities to better predict, prevent, respond to, and mitigate the effects of terrorism. The current threat environment mandates training courses that enable foreign countries to review and elaborate on the key elements and requirements for enhancing its information management capabilities.

Using ATA's systematic development methodology and Curriculum Development Guidelines, since 2006 GDIT worked on the following products for ATA:

- Critical Incident Management (CIM) Course
- Counter Terrorism Components of Academy Development (CTCAD) Course
- Hostage Negotiation (HN) Course and Course Rewrite
- Interdicting Terrorist Activities (ITA) Course and Course Rewrite
- Preventing Terrorist Attacks on Bus and Rail Systems (PTABRS) Course and Course Rewrite
- Protection of National Leadership (PNL — Revision of VIPP Course) Course
- Very Important Person Protection (VIPP) Course
- Protection of National Leadership Designated Defensive Marksman (PNL-DDM) Course
- Vital Infrastructure Security (VIS) Course and Course Rewrite
- Preventing Attacks on Soft Targets (PAST) Course Rewrite
- Tactical Support Team (TST) Course
- ATA collaborative SharePoint site and database

Courses included interactive instructional strategies and activities, such as firearms/range training, case studies, hands-on projects, threaded and capstone practical exercises, and scenarios that allowed participants to grasp and understand the course objectives. Course materials and deliverables included Course Description Guide (CDG) document, Facilitator Guide with detailed scripted instruction in a modularized format, Participant Guide, participant handouts, training aids (PowerPoint slides and other applicable training aids), course schedule, glossary of terms, knowledge and skills evaluations, pre-/post-course knowledge survey, End-of-Course Report (ECR), and concept equipment list. GDIT also provided expert content specialists and facilitators to support all the phases of each course development cycle to include Course Design, Lesson Module Development, Walk-Through, and Course Pilot/Rewrite Presentation.

As a result of our successful partnership with the ATA team, these courses received outstanding participant and facilitator feedback and demonstrated significant knowledge growth.

PROJECT NAME: DSS 0125 - EFFECTIVE COMMUNICATION IN DOD SECURITY
Value: $168,694
Duration: 2012 to present
Point of Contact: John Rizzo, Contracts POC, (410) 865-3245

Description: GDIT supported the design, development, and implementation of a 16-week graduate-level course titled Effective Communication in DoD Security. The course was designed to meet the requirements of the American Council on Education (ACE) for graduate-level credit equivalency at three (3) credit hours. Effective Communication in DoD Security covered effective techniques for communicating ideas, concepts, and policies in defense security. The course was designed to give mid-career security specialists in-depth knowledge, skills, and understanding of communication styles, concepts, principles, and theories of communication. Students use this knowledge and skill to become more effective as security leaders in the DoD.

GDIT developed instruction and activities in an interactive online collaborative learning environment (CLE). While students prepared project-based assignments independently, students also had the opportunity to learn and interact with other students in group discussions and by giving and receiving peer review feedback on course projects. The course included case studies and other methods of instruction that facilitated in-depth analysis of complex issues related to effective communication to support DoD security programs.

As a first step in the development process, GDIT conducted a comprehensive analysis of available written material and course topics to create a list of interview questions for DoD Subject Matter Experts (SMEs) in the area of security and communication. GDIT conducted and completed interviews of five DoD SMEs approved by the customer.

Once the interviews were completed, GDIT completed the following steps:

- Transcribed, analyzed, and mapped interview content to course topics.
- Researched and analyzed resources, publications, regulations, and Government-Furnished Information (GFI) to support content.
- Drafted course design plan including terminal learning objectives, a general description of course content, and instructional strategies.
- Developed detailed course design document including online interaction between the facilitator and participants and interaction between students using Sakai, an online Collaborative Learning Environment (CLE).
- Designed course content outline, course design plan, presentation method, Program of Instruction, syllabus, lesson plans, and evaluation criteria including graded student assignments and final project to evaluate mastery of the terminal learning objectives.
- Created assignments and assessment items, including rubrics and scoring guides, to evaluate student assignments.

- Developed lecture slides using customer-provided PowerPoint template. Enhanced instruction by providing high-resolution and colorful graphics, external links, facilitator audio narration, and transcripts of lecture slides. These items were added to address various learning modalities and adult learning strategies.
- Developed electronic files needed to present the course over the learning management system and collaborative learning environment used by the Center for Development of Security Excellence (CDSE).
- Facilitated the course using the approved final courseware including providing timely feedback and assessment of student assignments, timely response to student questions, and entering grades in the Sakai CLE.

Deliverables for this effort included the following:

- High-level course design plan
- Detailed course design document
- Assessment items
- Course material for presentation on CLE
- Beta iteration of course
- Beta test recommendations report
- Final courseware

As a result of our successful partnership with the DSS team, this course received outstanding participant and customer feedback and demonstrated significant knowledge growth. The **American Council of Education (ACE) reviewed and accredited the course** in its December 23, 2013, report, awarding college credit recommendation of three graduate-level credit hours for Effective Communication in DoD Security, allowing students to transfer credit toward Bachelor's or Master's degrees at many universities. Feedback from the ACE review team for the course included complements for the high quality of course design, course content, and documentation.

PROJECT NAME: NAVAL EDUCATION AND TRAINING PROFESSIONAL DEVELOPMENT AND TECHNOLOGY CENTER (NETPDTC) TRAINING PRODUCTS AND SUPPORT (NTPS)
Value: $57,510,649
Duration: 2008–2014
Point of Contact: Mike DeCoux, COR, (850) 473-6471

Description: GDIT provided ILT and WBT to the Naval Education and Training Professional Development and Technology Center (NETPDTC), resulting in hundreds of hours of online content and thousands of hours of instructional content. A total of 64 DOs were awarded via this Indefinite Delivery, Indefinite Quantity (IDIQ) contract; 42 of the DOs provided training content and 22 provided personnel support to multiple Navy training commands. These learning solutions reflect Naval Education Training Command / Integrated Learning Environment guidelines for standards, SCORM functionality, and Section 508 compliance. GDIT uses a variety of technologies to address the necessary enterprise-wide training requirements.

Complete List of Customers

Complete list of customers for whom the bidder has provided a similar commodities and/or services or with whom the bidder has contract with for the provision of similar commodities and/or services as those proposed in the response during the last two (2) years. The State 911 Department reserves the right to contact any and all customers set forth on the customer list:

Table 36 is a list of customers that General Dynamics has provided similar commodities and/or services or has contracted with for the provision of similar commodities and/or services as those proposed in the response during the last two (2) years.

Table 36. GDIT List of Customers that GDIT Supplied Applicable Services/Commodities to in the Last 2 Years

Customer/Contact Information	Similar Services Provided
Morgan County, Ohio David L. Bailey, 911 Coordinator (740) 541-9110 Davidlbailey10@embarqmail.com	Project: **Morgan County NG9-1-1** NENA i3-compliant NG9-1-1 production deployment for the State of Ohio (by county) with a fully functioning ESInet with spatial routing, based on geographic coordinates.
Federal Aviation Administration (FAA) Gloria Richmond, Technical Representative/COR (202) 267-7340 gloria.richmond@faa.gov	Project: **FAA Administrative Voice Enterprise Services (FAVES)** Architecture, design, engineering, transition, and operational management for an IP-based national converged voice communications network.
United States Coast Guard Gene Lockhart, R21 Deputy Program Manager (202) 475-3144 Eugene.g.lockhart@uscg.mil	Project: **National Distress and Response System Modernization Project (Rescue 21)** System design and development, site design and implementation, equipment installation at USCG Stations and Command Centers, and O&M support.
Defense Information Systems Agency (DISA) Marc Crandell, Program Manager, Hill AFB (801) 586-5559 marc.crandell.1@us.af.mil Marlon Mailey, Program Manager, HQ DISA Fort Meade (301) 225-2491 marlon.a.mailey.civ@mail.mil	Project: **DISA Wide Area Network Soft Switch (WANSS)** under the NETCENTS contract vehicle Engineer, Furnish, Install, and Test wide area network soft switches at multiple locations throughout the world providing converged Voice and Video over IP (VVoIP) and Unified Communications (UC) capability across the Defense Information Systems network (DISN) backbone.
Department of the Air Force Steve Ryder , Site POC, Telephone Maintenance Technician (907) 552-9700	Project: **E911 System at Elmendorf Air Force Base, AK** GDIT provided a complete JITC-certified upgrade to the current E911 system at Elmendorf Air Force Base, Alaska that included the installation of seven (7) Graphical User Interface (GUI) based E911 operator dispatch console positions; with each console equipped with two separate monitors (one for telephony and the other for LMR operation).

Customer/Contact Information	Similar Services Provided
Air Force Life Cycle Management Center Gerard Babauta, Program Manager, Unified Capabilities 801-586-3722 gerard.babauta@us.af.mil Jonathan Valle, Program Manager, Unified Capabilities 801-586-3865 jonathan.valle@us.af.mil	Project: **First Response** – E911 upgrades under the NETCENTS contract vehicle.at numerous AFB Including Joint Base McGuire-Dix-Lakehurst, Seymour Johnson AFB, Bangor ME Air National Guard, Lackland AFB and Goodfellow AFB. AF HQ/SAF has funded an Air Force–wide E911 program to address critical deficiencies identified in the "Air Force (AF) Follow-on Review; Protecting the Force: Lessons Learned from Fort Hood." The objective of this program is to provide for the purchase of the E911 Emergency Call Taking Systems that include E911 Intelligent Workstations (IWS) or Emergency Dispatch Positions and stand-alone ALI databases for multiple Air Force bases. The system support calls from on base PBX wire-line extensions (TDM and VoIP). The system shall provide the direct delivery of E911 calls to a DoD-staffed PSAP without the need for intermediate call answering by the local civilian PSAP.
East Orange Police Department, NJ Chief William Robinson, East Orange Police Dept (973) 672-4549	Project: **East Orange Police Department System Migration/Integration** GDIT provided installation, configuration, and training to replace an existing CAD/RMS application with GDIT's Law Enforcement Advanced Applications (LEAA) system,
Long Beach Island Michelle DeGeso, Chief of Communications (609) 494-3322	Project: **Long Beach Island (LBI)** GDIT built the first multi-agency CAD/RMS system to include data migration, installation, configuration, and training.
Jersey City Police Department (JCPD) John Tkaczyk, JCPD Sr. Systems Administrator (201) 547-5997	Data migration, installation, configuration, and training
U.S. Department of State (DoS) Bureau of Diplomatic Security Office of Antiterrorism Assistance (ATA) Dottie McCubbin, Operations Coordinator (571) 226-9710	Project: **DoS ATA Course Development Support:** Developed training courses and tools to enhance the capabilities of selected foreign governments' law enforcement and security forces.
Department of Defense (DoD) Defense Security Services (DSS) John Rizzo, Contracts POC (410) 865-3245	Project: **DSS 0125-Effective Communication in DoD Security** Design, development and implementation of 16-week, 3-credit graduate level course in an interactive online collaborative learning environment.
Naval Education and Training Professional Development and technology Center (NETPDTC) Mike DeCoux, COR (850) 473-6471	Project: **NETPDTC Training Products and Support** Provided Instructor-led training (ILT) and web-based training (WBT) resulting in hundreds of hours of online content and thousands of hours of instructional content.

Summary of the Qualifications and Experience of Subcontractors

A detailed summary of the qualifications and experience for each of the bidder's proposed subcontractor(s), including a listing of projects, similar in scope to that defined in this RFR, that each proposed subcontractor has participated in; and

GDIT assembled a team of qualified subcontractors based on their proven related experience and performance on projects similar to the scope they will be providing on the MA NG9-1-1 project. Each of our teammates has been active in the design and developed of NG9-1-1 products and services and have served on various standards committees related to NG9-1-1. We will apply our

shared experience of past successes to deliver an on-time, quality system to the Commonwealth of Massachusetts.

SYNERGEM

Founded in 2001, Synergem is a privately held company providing intelligent Next Generation 9-1-1 solutions with its Evolution911™ line of products across the emergency communications spectrum. In its home state of North Carolina (NC), Synergem is a regulated Competitive Local Provider (CLP, a title unique to NC that is equivalent to a CLEC in other parts of the nation).

For the MA NG9-1-1 project, Synergem will be providing the Emergency Routing Service proxy (ESRP), Legacy Network Gateway (LNG) and Legacy PSAP Gateway (LPG).

Synergem clearly understands NENA's requirements. They were the first provider of an Emergency Services IP Network (ESInet) designed and provisioned in accordance with the requirements of NENA 08-003, the Detailed Functional and Interface Specification for the NENA i3 Solution; the first to route an end-to-end SIP call through that network, and to have its ESInet acceptance tested in NC.

Today, Synergem exclusively operates in the public safety, emergency communications sector governed by NENA and the Association of Public Safety Communications Officials (APCO) performance standards and objectives. Synergem provides a carrier-grade Emergency Services IP Network (ESInet). This solution leverages technologies consistent with NENA i3 specifications that support multiple integrated applications and data management services.

The company collaborates on the development and distribution of its solutions within a technical partnership that includes NACR, Affiliated Communications, Avaya, Oracle, ArrowS3, General Dynamics, and others. This partnership allows Synergem to ensure its customers get the personal attention of a small company and the almost unlimited array of products available through the largest suppliers. GDIT teammates Oracle and Synergem have a very close working relationship and jointly participate in ICE sessions demonstrating a variety of industry leading integration capabilities that are critical for NG9-1-1.

On June 9, 2011, Synergem Technologies successfully routed the Nation's first "NENA i3" end-to-end call through its ESInet. The end-to-end call originated in Winston-Salem, NC on Windstream's Private Switched Telephone Network (PSTN) and delivered through a Session Initiated Protocol (SIP) trunk connected to Synergem's EvolutionNET™ ESInet. EvolutionNET™ "geospatially" routed the call to the Winston-Salem Police Department (WSPD) where it was answered on Synergem's Evolution911™ SIP-based call-taking application. In order to verify the ESInet could dynamically reroute calls to another center, to simulate an action that would be required if the WSPD PSAP was offline, the team changed the routing policy by using a graphical map interface to draw a polygon around WSPD's jurisdictional boundary. As a result of this change, when another call originated from within the WSPD's jurisdiction, it was automatically geospatially routed to the 9-1-1 center in Surry County, NC.

This end-to-end call was part of the exhaustive EvolutionNET™ acceptance testing program that marked the successful completion of the year-long provisioning phase of this project. The North-Central North Carolina Compact, which was an agreement developed among multiple

governmental entities, demonstrates the ability of the Synergem team to act as a provider of end-to-end emergency communications solutions for organizations of all types and sizes.

The following is a listing of projects, similar in scope to that defined in this RFR, that Synergem has participated in:

PROJECT NAME: SPRINK COUNTY SD, SHERIFF'S OFFICE
Duration: 6/2004 – ongoing
Point of Contact: Marleen Huckaby, E9-1-1 Supervisor, (605) 472-4595, spinkcountyso@midconet.com

Project Description: Installed ANI/ALI software and hardware and upgraded radio. Have supported and maintained equipment to present. Now installing NG9-1-1 call-taking solution (**Evolution911™**) with go-live date mid- to late January, 2014.

Equipment and/or products maintained, installed, implemented, or other: Synergem ANI/ALI Delivery System (Precursor to Evolution911™). Now installing Evolution911™.

Related Services performed: Provided background briefings for county officials and other service providers. Helped to find a source of funding.

Professional Services performed: Design, procurement, installation, testing, and support and maintenance.

Training Services performed: Provided complete training package covering all aspects of software and hardware.

Relevant Scope to RFR: Involves products proposed in MA.

PROJECT NAME: MARENGO COUNTY AL EMERGENCY MANAGEMENT AGENCY
Duration: 6/2007 – ongoing
Point of Contact: Kevin McKinney, Director, (334) 295-8870, marengoema@bellsouth

Project Description: Installed and maintained E9-1-1 ANI/ALI controller. Migrated agency to ***Evolution911™ Call-taking application***. System went live in December, 2013. Now in maintenance and support mode.

Products maintained, installed, implemented, or other: Synergem ANI/ALI Delivery System (Precursor to Evolution911™) until 12/13. Now Evolution911™

Related Services performed: Provided background briefings for county officials and other service providers.

Professional Services performed: Design, procurement, installation, testing, and support and maintenance. Integrated system with other legacy applications.

Training Services performed: Provided full range of call taker training relative to new installation.

Relevant Scope to RFR: Involves products proposed in MA.

PROJECT NAME: NORTH CENTRAL CAROLINA NG9-1-1 COMPACT WINSTON-SALEM POLICE DEPARTMENT

Duration: 1/2010 – 6/2011

Point of Contact: Julia Conley, IT Director, (336) 391-4415, juliac@wspd.org

Project Description: provisioned **EvolutionNET™**, an ESInet developed consistent with i3 standards and offered it as software as a service (SaaS). System accepted in 6/2011. Routed nation's first end-to-end i3 call via network.

Products maintained, installed, implemented, or other: EvolutionNET™, i3 compliant ESInet

Related Services performed: Wrote and processed $2.4 million grant awarded by state. Provided background briefings for city officials and other service providers.

Professional Services performed: Design, procurement, installation, testing, and support and maintenance. Integrated system with other legacy applications.

Training Services performed: Provided full range of call taker training relative to new installation.

Relevant Scope to RFR: Involves products proposed in MA.

EMERGENCY CALLWORKS

Emergency CallWorks (ECW) was founded in 2006 to develop and market a next generation, dispatch-centric emergency call taking and dispatch system. The solution combines Enhanced 9-1-1 Call Taking (NG9-1-1), Integrated Mapping (Mapped ALI) and Dispatch System (CAD) capabilities into a single source solution for the small to mid-sized emergency call taking and dispatch environment.

Emergency CallWorks was selected by GDIT to provide the Customer Premise Equipment (CPE) which includes the IP Automatic Call distribution (ACD) solutions as well as the PSAP position call taking interface. ECW's solution is web-based, offering a centralized approach to CPE, a solution that will provide the Commonwealth significant capability and flexibility while reducing ongoing operational costs.

ECW provides the Public Safety Answering Point (PSAP) and Dispatch community with the industry's first fully integrated solution for Next Generation 9-1-1 call taking, mapping, dispatching of resources, and consolidated reporting while providing a vast array of benefits from VoIP and web-based technology. Emergency CallWorks products improve control and administration of the E9-1-1, Emergency Management and Dispatch workflow process while enhancing the speed and accuracy of emergency response.

Emergency CallWorks applications enable more efficient call taking and dispatch operation, comply with FCC mandates for wireless E9-1-1 calls, accommodate non-traditional communications and resolve aging legacy support issues many agencies face today. The systems can also be deployed in E9-1-1 Call Taking or Dispatch only or mixed use configurations. ECW offers both in any combination needed.

These highly integrated capabilities provide the most cost-effective solution for small to mid-size Public Safety Answering Points (PSAPs) and Public Safety Dispatch centers across North America, yet can easily scale upwards into the largest Dispatch environments all while primarily utilizing Commercial Off-the-Shelf (COTS) hardware.

Emergency CallWorks has participated in multiple NG9-1-1 demonstrations (ICE, ANGEN) that proved our technology successfully interfaces to i3 Networks and interconnects to other vendor and carrier solutions.

The following is a listing of projects, similar in scope to that defined in this RFR, that Emergency CallWorks has participated in:

PROJECT NAME: SOUTHWEST OKLAHOMA REGIONAL 9-1-1 ASSOCIATION, OK

Duration: System cutover to live operations in December 2011
Point of Contact: Jana Harris, 911 Director, (580) 562-4882 ext 137, Jana@swoda.org

Project Summary: The Southwest Oklahoma Regional 9-1-1 Association needed to not only improve the call taker workflow, processing speed, and overall efficiency but also improve overall public safety while reducing ongoing operating costs.

Relevant Scope to RFR: The ECW CallStation solution includes 18 CallStation Positions located in 12 locations throughout the region. Deployed in a Geo-Diverse (multi-site) and "N" scalable server configuration for potential growth and geographical flexibility.

PROJECT NAME: MUSKOGEE CITY / COUNTY TRUST AUTHORITY, OK

Duration: System cutover to live operations in July 2011
Point of Contact: Darryl Maggard, 911 Coordinator, 918 984 8641, Darryl@mcc911.org

Project Summary: The Muskogee City/County Trust Authority (MCCE911TA) sought to implement a Next Generation 9-1-1 telephony solution to enhance emergency response and better protect its residents of Muskogee County, its twelve towns and the City of Muskogee. In addition, the system merges five separate dispatch centers, including Muskogee Police, the Muskogee County Sheriff's Office, Muskogee EMS, and the Muskogee County Fire Department, into one consolidated communications center.

Relevant Scope to RFR: The MCCE911TA installed Emergency CallWorks' Next Generation E9-1-1 call taking solution. The center consists of eight (8) positions and includes: Next Generation-ready 9-1-1, CAD spill to New World Systems, and headset integration to the Motorola radio system. In addition, DecisionStation allows MCCE911TA to easily manage reports and remote monitoring.

PROJECT NAME: JEFFERSON COUNTY, AL

Duration: Completed February 2014
Point of Contact: Howard Summerford, Director, 205 520 9967, summerfordh@jeffcoal911.org

Project Summary: The largest county in Alabama, Jefferson County, with an estimated 660,000 citizens, selected Emergency CallWorks (ECW) to supply advanced 9-1-1 call management and

call mapping. The new system, built to meet and exceed the latest Next Generation (NG) 9-1-1 standards, will help improve emergency response capabilities, consolidate operations, and add efficiencies as well as lower technology and operational costs.

Relevant Scope to RFR: The new NG9-1-1 call management solution will be deployed with the capability to service all of the existing Public Safety Answering Points (PSAPs) within the County. The Jefferson County Emergency Communications District serves all of unincorporated Jefferson County plus 18 incorporated cities and towns. This includes the Jefferson County Sheriff's Office, nine other law enforcement agencies, and 33 fire/EMS agencies across the county. The solution will be deployed in an easily scalable, geo-diverse, multi-site environment with flexibility and capacity to handle community growth, consolidation strategies, and geographical or disaster recovery situations.

WINDSTREAM

Windstream will be the GDIT team Local Exchange Carrier (LEC) providing data center facilities, MPLS network, and connectivity to/from all PSAPs. Windstream is the fourth-largest telecommunications company in the United States and has been doing business for 72 years. Windstream is one of the U.S. government's most trusted communications providers – supporting more than 150 clients that include the White House Communications Agency, State Department, Internal Revenue Service (IRS), Defense Information Systems Agency (DISA), National Aeronautics and Space Administration (NASA), and more. Windstream data center facilities are state-of-the-art high-availability data centers and have extensive experience working with the Commonwealth.

The following is a list of projects showing network and installation experience similar in scope to that defined in this RFR, that Windstream has participated in:

PROJECT NAME: COMMONWEALTH OF MASSACHUSETTS INFORMATION TECHNOLOGY DIVISION (ITD) MAGNET PROJECT
Duration: 2007 – present
Point of Contact: Brad Steele, Director of Unified Communications, 617-626-4645, brad.steele@state.ma.us

Description: 60+ site MPLS/SIP deployment. Initial deployment was processed and scheduled within window of 120-180 days. Upgraded incumbent network to MPLS and deployed several mediums including T1, nxT1, and Ethernet. As part of this deployment, Windstream successfully transitioned many State agencies away from legacy PBX and TDM voice networks to the ITD Shared Switch SIP environment. Since initial deployment, Windstream has added several new sites as well as completed necessary moves for relocating offices. Windstream has successfully upgraded several HUBs and remotes to new circuits in order to meet demands for increased capacity and QnQ capabilities.

This strategic design includes CO and last mile redundancy including plans for multiple failover scenarios for voice and data. Attributes of the network include multiple SIP trunk groups supporting g.711 and g.729, BGP, and static routing as well as multiple secure VRFs containing several different QoS mappings.

PROJECT NAME: COMMONWEALTH OF MASSACHUSETTS TRIAL COURTS

Duration: 2008 – present

Point of Contact: Customer requires written request for release of this information

Description: 120+ site MPLS network. Initial deployment was processed and scheduled within window of 120-180. Replaced and upgraded incumbent network to MPLS via T1, nxT1, and Ethernet. This network is carrying mission-critical information that requires resiliency due to security concerns with the Courts. Throughout the support of this network, Windstream has added bandwidth and redundant facilities and upgraded several sites to Ethernet to meet increased bandwidth demands of the customer for voice and video. Windstream has worked hand-in-hand to project manage Court moves that were both temporary and permanent while keeping the network functioning as needed. Design scope included careful planning for CO and last mile redundancy. Deployment was managed with the highest integrity to ensure end users did not notice the transition. Network includes BGP and static routing while maintaining several different queues for QoS. Due to being part of the Commonwealth, the network is managed by our Elite Emergency Response Center, which is a subset of Windstream's top Emergency Response Communications (ERC) technicians who only manage our largest clients.

PROJECT NAME: STATE OF NEW YORK, OFFICE OF TECHNOLOGY

Duration: 2008 – 2017

Point of Contact: Kim McKinney, Chief Operations Officer, (518) 402-7000, kim.mckinney@cio.ny.gov

Description: Windstream provides Telecom, Internetworking, MPLS backbone for State of NY featuring Cisco Core Routers supporting OC-48 Ring and Adtran switching MUX for transport down to office sites. The Office for Technology for the State of New York was buried in 15-year-old telecommunications infrastructure, decentralized among multiple carriers, resulting in uncompetitive rates and logistical issues. The State's voice communications platform, known as CapNet, supplied 64,000 State employees with voice services both locally in the Capital District as well as to regional locations across the State. In just four short months Windstream designed, configured, installed, and migrated nearly 70,000 State DIDs onto a private OC-48 ring using Cisco Systems' Optical Network Systems (ONS) ring and seven Regional PBX locations (Binghamton, Buffalo, Syracuse, Rochester, NYC, Poughkeepsie, and Long Island) connected via Windstream's TDM infrastructure. This provided the State with a single carrier for both local and long distance, a local dedicated Account Team, which remains in place today, and state-of-the-art infrastructure with marked improvements in service delivery for both voice and data services including SIP trunking. Windstream accomplished all this while still providing an initial savings of $360,000 per year, which has now grown to over $890,000 per year to date. Today Windstream is moving forward with upgrading the infrastructure to Dense Wavelength Division Multiplexing (DWDM) to support transport services at 10 GE and higher.

PROJECT NAME: MIAMI-DADE COUNTY PUBLIC SCHOOLS

Duration: 2006 – present
Point of Contact: Mr. Glenn J. Tekerman, Manager of Contracts and Financial Services, 305.995.3723, gtekerman@dadeschools.net

Description: Windstream has installed over 300 Avaya S8300 Call Managers in the past four years. We designed configurations from very small (50 – 60 ports) for early learning centers/elementary schools to very large (over 500 ports) for regional super high schools. The Avaya systems are replacing Nortel Norstars and Option 11s and include Windstream moving/ extending the MFD, adding power (110v and 220V), doing the wiring and jacks in the classrooms, and programming and installing the S8300 with voice mail and a 6KVA UPS. Most recently the customer has made a decision to move to the Avaya IP Office platform and has purchased the first 30 systems of a 106 system e-Rate rollout, installed between February 2013 and June 30, 2013. This followed a "test" VoIP IP Office installation at the Medical and Science Technology (MAST) School in 2012. This system has been so successful, the customer submitted e-Rate Y16 applications for 100+ additional IP Office systems in 2013. Windstream also maintains both the CM and IP Office systems under a special, e-Rate eligible contract. Avaya provides monitoring only and reports troubles to Windstream, who dispatches the engineer for repair.

PROJECT NAME: EL PASO INDEPENDENT SCHOOL DISTRICT, VOICE NETWORK UPGRADE

Duration: 2011 – present
Point of Contact: Jessica Herrera, Director, Network Services, (915) 887-5469, jsherrer@episd.org

Description: Upgrade of a core site from 20-year-old Avaya/Nortel equipment to three-site redundant PBX network core. Currently upgrading 98 remote locations to support in excess of 8,000 digital, analog, and IP handsets on an all-IP backbone made up of Cisco equipment. Also contracted for maintenance.

PROJECT NAME: SPRINGFIELD, MASSACHUSETTS HOUSING AUTHORITY

Duration: 2011 – present
Point of Contact: Stephen Ethier, IT Manager, 413-787-9844, sethier@shamass.org

Description: Provided, deployed, and support ShoreTel UC/VoIP System for multi-site SHA office throughout the Greater Springfield region.

PROJECT NAME: NC WILDLIFE

Duration: 9/1/2006 – present
Point of Contact: Janice Underwood, 919-707-0007, Janice.underwood@ncwildlife.org

Description: NC Wildlife contracted for a Private Cloud solution with Windstream. It includes servers, storage, network gear, IDS/IPS, Load Balancing, VMware, and Windows licensing and management.

PROJECT NAME: MASSACHUSETTS LEGAL ASSISTANCE CORPORATION
Duration: 6/1/2007 – present
Point of Contact: Tobey Johnson, 619-367-1414, tjohnson@legalservicesma.org

Description: Two cabinets of collocation with Internet bandwidth.

DSS CORPORATION

DSS Corporation has been in business for over 40 years with more than 20 years in the public safety industry. DSS experience includes a national installed base of over 1,000 PSAPs including 270 PSAPs with the Massachusetts State 911 Department. Their Chief Technologist chairs the NENA steering committee and sits on NG9-1-1 i3 standards committee, and DSS has participated in every NENA Industry Collaboration Event (ICE).

DSS will be providing the Digital Logging Recorder (DLR) solution for this project. They have managed Massachusetts S911D digital logging recorders from a successfully expedited installation schedule to current maintenance of all ~255 current PSAPs.

The following is a listing of projects, similar in scope to that defined in this RFR, that DSS Corporation has participated in:

PROJECT NAME: MASSACHUSETTS STATE 911 DEPARTMENT
Duration: January 2012 – present
Point of Contact: Trish Pries, Project Manager, 508-821-7206, tricia.pries@state.ma.us

Description: 270 PSAPs for the City PD, Sheriff, Fire Departments, and State Police. All included ANI/ALI data integration and proactive 24/7 monitoring. Equipment provided on this project is NG9-1-1 compatible, upgradable on demand.

PROJECT NAME: COLORADO STATE PATROL
Duration: June 2011 – present
Point of Contact: Don Naccarato, 719-288-2622, don.naccarato@cdps.state.co.us

Description: Multi-site public safety project that includes standard recording technologies along with video and multi-media recording. DSS maintains full support and monitoring requirements while meeting stringent on-site requirements.

- Multi-site Public Safety that includes video security recording
  - 100 video inputs across four sites
- MCC 7500 version 7.13 current integration
- Proactive 24x7 monitoring

Relevant Scope to RFR: Multi-site, multi-media public safety environment.

PROJECT NAME: WEST CENTRAL TEXAS COUNCIL OF GOVERNMENTS

Duration: March 2012 – present

Point of Contact: Joe Rogers, 325-672-8544, jrogers@wctcog.org

Description: Multi-site (18) public safety environment that includes city, sheriff, and PSAP agencies. DSS maintains and monitors the systems and requisite NG9-1-1 compatibility for future enhancements. Multi-site public safety environment that required NG9-1-1 capability, proactive 24x7 monitoring, and managing disparate PSAPs and agencies.

DIGITAL DATA TECHNOLOGIES, INC. (DDTi)

Since 1993, DDTi has been providing state-of-the-art spatial solutions to both the public and private sectors. DDTi developed a highly efficient and accurate methodology for field verified GIS data collection that is able to serve the diverse needs of state, county, and municipal governments. Their unique approach was recognized as a Best Practice by the U.S. Department of Transportation in its 2011 Transportation for the Nation strategic plan.

DDTi is providing the Geographical Information System (GIS) solution including the ECRF/LVF for the MA NG9-1-1 project. DDTi has more than 10 years of experience implementing multi-site 911 systems that includes over 1,000 installations across the U.S. with more than 150 installations in PSAPs nationwide. DDTi is the only company recognized by NENA with a certificate of appreciation for outstanding contribution made to the ECRF/LVF i3 standards. DDTi, like our GDIT teammates Oracle and Synergem, participates in ICE sessions to help establish NG9-1-1 standards and demonstrate proven functionality and interoperability.

DDTi has conducted over 200 GIS data reviews and analyses that examined map data problems that could potentially cause data synchronization issues. With their precision Data Validation process, DDTi analyzes existing data using 35 different tests to uncover potential or suspected map data issues that may impede accurate address location. Their process ensures uniformity, accuracy, and adherence to National Emergency Number Association (NENA) standards (71-501).

DDTi has performed data collection in over 80 jurisdictions and their compilation methodology is the most thorough, accurate, and reliable available. DDTi GIS professionals drive every public and private road in a jurisdiction and utilize innovative mobile mapping technology that combines three navigation technologies with a revolutionary voice recording system. DDTi's field-verified data is accurate to +/- 1 meter and conforms to National Emergency Number Association (NENA) standards (02-014).

Created with the Public Safety Answering Point (PSAP) environment in mind, DDTi's Dispatch software product empowers dispatchers to identify caller locations and assist in the transfer of information to first responders and is installed in over 400 PSAPs. DDTi's Mobile Command Center, featuring integrated Automatic Vehicle Location (AVL) capabilities, empowers authorized users to precisely track information about their Police, Fire, EMS, and other agency assets. This software services is tracking thousands of vehicles nationwide.

DDTi continues to work closely with NENA to develop standards and protocols for Next Generation 9-1-1, including provisioning and maintenance of GIS to the ECRF/LVF, i3 architecture considerations, and development of the Forest Guide. DDTi has participated in

NENA's Industry Collaboration Events (ICE 3, ICE 4, ICE 5, and ICE 8) and is proud to have been recognized by NENA with a certificate of appreciation for our outstanding contribution to the development of ECRF/LVF i3 standards.

DDTi's Next Generation 9-1-1 functional elements are designed to comply with existing IETF and NENA standards, and to be interoperable with all other functional elements adhering to those same standards.

The following is a listing of projects, similar in scope to that defined in this RFR, that DDTi Corporation has participated in:

PROJECT NAME: MORGAN COUNTY NG9-1-1
Duration: 12/2013 – 12/2016
Point of Contact: David Bailey, 9-1-1 Coordinator, 740-541-9110, davidlbailey10@embarqmail.com

Contract Number: Multiple contracts

Contract Nature: Subcontractor to GDIT for ECRF/LVF and LIF software for hosted NG9-1-1 solution. Direct contractual relationship for website hosting, GIS data maintenance, dispatch software, and software support.

Project Summary: Installation of ECRF/LVF, Data Normalization Services, Transitional ALI software (LIS).

Relevant Scope to RFR: Live installation of key NG9-1-1 components including ECRF/LVF, LIF, and data normalization.

PROJECT NAME: MORGAN COUNTY NG9-1-1 (IN SUPPORT OF GDIT)
Duration: 12/2013 to 12/2016
Point of Contact: David Bailey, 9-1-1 Coordinator, 740-541-9110, davidlbailey10@embarqmail.com

Description: Subcontractor to GDIT for ECRF/LVF and LIF software for hosted NG9-1-1 solution. Responsible for installation, including live installation of key NG9-1-1 components including ECRF/LVF, LIF, and data normalization. Direct contractual relationship for website hosting, GIS data maintenance, dispatch software, and software support.

PROJECT NAME: SHELBY COUNTY SHERIFF'S OFFICE NG9-1-1
Duration: 12/2013 to 12/2016
Point of Contact: Patrick Goldschmidt, 9-1-1 Coordinator, 937-494-2108, patrick.goldschmidt@shelbycountysheriff.com

Description: Responsible for installation, including live installation of key NG9-1-1 components, including ECRF/LVF, LIF, and data normalization. Direct contractual relationship for website hosting, GIS data maintenance, dispatch software, and software support.

PROJECT NAME: NG9-1-1 LBRS (LOCATION BASED RESPONSE SYSTEM) – STATE OF OHIO (SUBCONTRACTOR TO GDIT)
Duration: 9/13/13 – 6/30/15
Point of Contact: Jeff Smith, OSDI Manager, Ohio Geographically Referenced Information Program, 614-466-8862, jeff.smith@das.ohio.gov

Description: Subcontractor to GDIT for ECRF/LVF and LIF software for hosted NG9-1-1 solution. Direct contractual relationship for GIS data maintenance, dispatch software, and software support.

Role of Key Equipment Vendors

Oracle will be providing their Session Border Controller (SBC) solution, performing as the ESInet Border Control Function (BCF). Oracle's products have been delivering mission-critical multimedia applications, including voice implementations in virtually every Tier I service provider worldwide, for 12 years. Ninety-two (92) of the top 100 carriers deploy Oracle's VoIP-enabled solutions. These products are globally deployed and support emergency 911 services traffic for the U.S. government, the U.S. military, and the largest enterprises and financial institutions. Oracle participates in multiple ICE sessions and helps define many of the current and future NG9-1-1 standards.

Aculab will be providing the Protocol Interworking Function (PIF), which is the functional component of the LNG that interworks legacy PSTN signaling such as ISUP or CAMA with Session Initiation Protocol (SIP) signaling. Oracle, Synergem, and Aculab have an extremely close working relationship that has culminated into an industry leading LNG solution that is proven time again at various ICE sessions.

Cisco is a key equipment provider for this project. We will use the Cisco Security Manager, a comprehensive management solution that enables advanced management and rapid troubleshooting of multiple security devices. Cisco will also be providing routing, switching, firewalls. The Cisco components will help ensure that only authorized communications will be available over the network.

Other Information

Any other information the bidder considers relevant and supports stated experience and expertise.

Not applicable.

Summary of Qualifications and Skills

A detailed summary of qualifications and skills of the bidder and all key personnel identified by the bidder who will perform services as set forth in this RFR, including the specific knowledge and experience of each individual in the area of public safety communications (distinguishing between administrative staff, management, principal partners or officers, field, technical and customer support), including for NOC personnel;

An organizational chart for the project listing each individual who will be assigned to perform services as set forth in this RFR, and a description or listing of the planned role and work for each individual;

A proposed Contract Manager who will be responsible for oversight and management of contract performance and shall act as the primary contact person for receipt of notice and other communications under the contract, including

but not limited to, timely reports and written responses and attendance at meetings as required by the State 911 Department;

A proposed Project Manager, who shall be a certified PMP, with a minimum of ten (10) years experience managing large projects, and include his/her resume including a listing of relevant projects;

A main tenet of GDIT's project management is "no surprises." We are committed to the project goals and believe that open communication is the best policy to promote the broadest level of customer satisfaction. In addition to providing a technically sound solution, GDIT will provide a senior management team to ensure the complete success of the installation, support, and sustainment.

The GDIT Program Management Office (PMO) will support the project management, engineering, operations, contractual, and financial actions necessary to sustain the Project Manager and deliver the installation, support, and sustainment on schedule and on budget. The PMO structure and reporting is designed to promote proactive task management at all levels of the organization. Because of the complexity and magnitude of the MA NG9-1-1 project, we have also appointed a Project Director, Ms. Joan Newlon, to support the overall Project Manager, Mr. Paul Chotkowski. Ms. Newlon is, a senior manager with extensive network, unified communications, production, and infrastructure deployment experience. Ms. Newlon today has responsibility for all NG9-1-1 and USMC and Navy Voice Infrastructure programs in the GDIT Unified Communications Organization. On upon award of the program, this will be Ms. Newlon's primary responsibility.

Our entire leadership team will report through a single management chain to eliminate organizational boundaries. Ms. Newlon and Mr. Chotkowski, will have full and immediate access to executive management, namely Mr. John Walsh, Vice President of GDIT's Unified Communications organization. As shown in Figure 98, Mr. Chotkowski will oversee and manage all MA NG9-1-1 implementation, operation, and engineering activities, to include managing and integrating our subcontractor and OEM activities to ensure our team meets an on-time delivery.

We have worked with our partnering companies and have mutually agreed to assigned roles and responsibilities of the team, as described in Section 8.9, Project Management. This ensures a clear understanding between team members, allows us to hit the ground running, and results in no gaps or overlaps during performance.

The GDIT team will collaborate with the Commonwealth using a highly experienced team drawing the most qualified expertise from our team members. Our Project Manager and engineers are part of a delivery team optimized to ensure performance on all Milestones. Additional Key Personnel are identified below, and resumes follow.

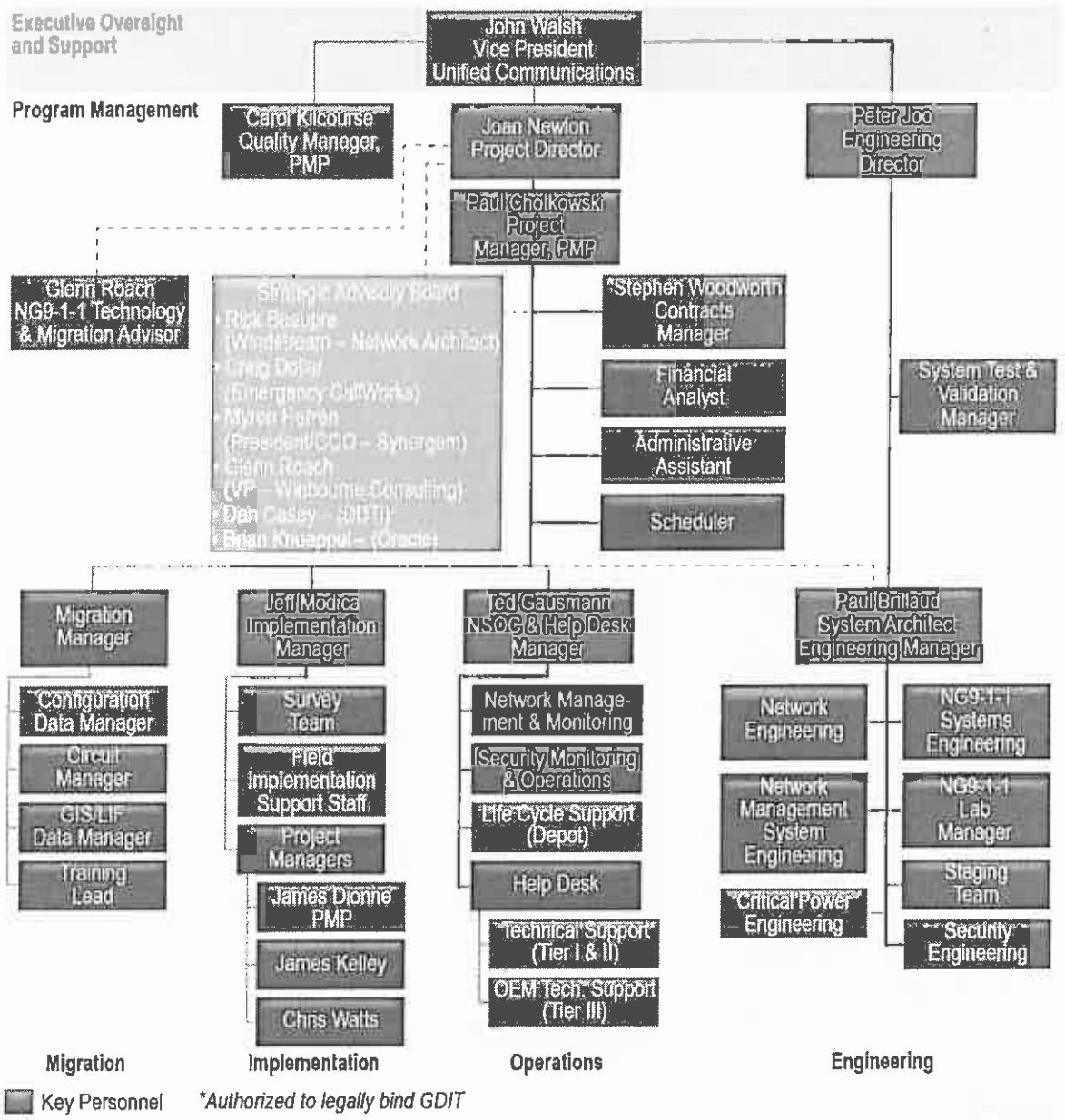


Figure 98. GDIT Commonwealth of Massachusetts NG9-1-1 Project Organizational Chart

In addition to the key personnel identified in Table 37, our team has a large pool of qualified, experienced professionals who will be assigned to this project. Our team has significant depth and reach when it comes to designing, implementing, and supporting large-scale projects similar in nature to the MA NG9-1-1 project. As such, we are able to efficiently staff projects like these with the appropriate skill sets to ensure successful and timely delivery and contract performance. GDIT's program management team of highly experienced personnel has the experience, certifications, and skill sets to meet the requirements of the Commonwealth.

Table 37. GDIT Team Key Personnel

Key Team Members	Responsibility	Qualifications
Joan Newlon, Project Director	Overall responsibility for the project, including partner and financial management, quality assurance, and escalation to executive management	• 25+ years' experience managing large complex network, unified communications, production, and infrastructure deployment projects • Extensive production operations and processes experience will be applied to optimizing PSAP configuration, test, burn in, and deployment • Extensive experience managing multiple subcontractors in large-scale deployments • BSEE, MBA, and Graduate of Defense System Management College for Program Management
Paul Chotkowski, PMP, Project Manager	Primary interface with the Commonwealth and project personnel, and overall responsibility for managing day-to-day operations including product and services delivery, supervising personnel, and status reporting	• More than 15 years of project management experience, including the Colorado Springs Command Post Consolidation and the McGuire E911 Integration • Six years of public safety–related project management experience directly related to E911 technology and processes • Successfully managed over 15 E911 PSAP projects at various Air Force bases throughout the U.S.
Stephen Woodworth, Contracts Manager	Responsible for oversight and management of contract performance and will act as the primary contact person for receipt of notice and other communications under the contract	• More than 20 years of contract experience • GDIT contracts manager for State of New York Statewide Wireless Network project • BS, ABA approved Comprehensive Paralegal Certificate
Glenn Roach, Transition/Migration Liaison	Coordinate transition/migration and implementation activities Serve as a point of contact between the carriers (Verizon, CLECs, Wireless, VoIP, etc.), Commonwealth, PSAPs, and GDIT staff and partners	• 20+ years of experience in public safety emerging technologies and Next Generation Services (NG9-1-1) • Expertise includes 9-1-1 and public safety communications planning, administration, operations, technology, regulations and legislation at the international, federal, state, and local level • 30+ years of experience in drafting and administering standard operating procedures for telecommunications, call centers and public safety communications • Played a major role on public safety communications related standards setting bodies to include NENA, ESIF, and ATTIS; recently involved in the National Public Safety Broadband effort with FirstNet • Certified Emergency Number Professional (ENP)
Paul Brillaud, System Architect	Responsible for the end-to-end system architecture for the Massachusetts NG9-1-1 project	• 23 years of success delivering technology solutions to government and enterprise markets, articulating strategic technology vision, and building business efficiency for emerging technology products and services • Technical depth in converged IP services (voice, video, data), including cloud services, infrastructure, UC, NG9-1-1 operations support, and cyber security • Team lead for project, architectural, and implementation engineering to achieve business and technical performance and project success

Key Team Members	Responsibility	Qualifications
Jeff Modica, Implementation Manager	Responsible for the day-to-day management of Implementation efforts, including project schedules, training, testing, and cutover	• Over 17 years of engineering and program management experience deploying DoD telecommunications systems • Senior Technical Director for numerous successful programs • BBA
Ted Gausmann, Operations Manager	Leads all efforts related to the operations and maintenance of the delivered solutions (help desk, customer service center, trouble ticketing, and reporting, NOC staff, etc.)	• 25 years of program/project management, primarily in telecommunications and Information technology services • Manager of 24x7x365 NOC providing technical support services to field technicians and end users • Technologies supported include voice switching systems, networks, and related equipment; enterprise VoIP systems; and E911 systems
Peter Joo, Engineering Manager	Overall responsibility for design and management of all engineering resources	• Designed USAF Enterprise 9-1-1 for public safety, including 170 PSAPs, hosted data center design, regionalized PSAP design, and NG9-1-1 pilot
Carol Kilcourse, PMP, Quality Manager	Overall responsibility for Quality Management	• Over 18 years of experience in program and project management, including 5 years in her current role as GDIT's Project Control Manager

Key Personnel Resumes

PROJECT DIRECTOR – JOAN NEWLON

Ms. Newlon is a highly skilled, results oriented professional with 25+ years of proven program and operations management experience in the telecommunications and IT industries. Ms. Newlon is a progressive leader with strong team building skills, and provides broad experience and proven performance in Program and Project Management, Proposal Management, Operations Management, and Engineering. Ms. Newlon has demonstrated repeated successes in effectively managing multi-million dollar complex projects within scope/cost/and schedule while ensuring customer satisfaction and company profitability. Ms. Newlon possesses strong technical background, bridged with exceptional communication, interpersonal and leadership skills.

CAREER SUMMARY

General Dynamics, 1984–Present

Director – Unified Communications, 2006–present
Complete responsibility for Program Management of all USMC and Navy Voice projects in Unified Communications Organization. Programs managed combined value $200M+ for Unified Communications Upgrades and Regional Telecommunications Management Systems at 17 CONUS and 12 OCONUS U.S. Navy and USMC sites.

Program Manager – Base Level Information Infrastructure Program (BLII), 2005–2006
Overall responsibility for managing a $150M+ program for designing, engineering and installing the data networks and network infrastructures at 16 OCONUS U.S. Navy sites in support of 35,000 users.

Managed seven first-tier subcontractors for both infrastructure work and network integration utilizing a variety of contract types. Interfaced with multiple vendors and second-tier subcontractors in the performance of this contract.

Far East Regional Manager – Base Level Infrastructure Program (BLII), 2003–2005
Responsible for managing 9 of 16 areas of the BLII program representing 70% of the work of a $150M+ program. Extensive travel to Japan, Korea, Guam.

Hired and directed 30+ field personnel assigned as Site Managers, OSP, ISP, and Network Leads.

Managed three first-tier subcontractors for both infrastructure work and network integration, and developed program subcontract Statement of Work templates and negotiated all subcontract agreements.

Developed and negotiated BLII program wide pricing model incorporated into the contract by the customer for pricing all contract scope changes.

Program Manager – Base Telecommunications Infrastructure Upgrade, 2000–2003
Overall operational and financial responsibility for network infrastructure design and implementation program for the U.S. Marines at 9 Marine bases in Japan.

Developed program subcontract Statement of Work templates and negotiated all subcontract agreements.

Managed three first-tier subcontractors and developed performance metric model for tracking and managing work performed to schedule and cost. Met or exceeded customer schedule requirements, exceeding all program financial goals, while achieving 100% Customer Satisfaction rating.

Program Manager – Wire and Cable Services Program (WACS), 1998–2000
Complete P&L responsibility for a large multiple award IDIQ GSA contract open to all federal agencies for telecommunications infrastructure.

In first year of contract developed sales opportunities that resulted in the submittal of over 100 proposals to several federal agencies.

Established several subcontractor agreements with infrastructure installation small businesses to ensure nationwide coverage capability.

Developed a program staff of sales, marketing, engineering, proposal development, project management, finance, and contracts personnel.

Program Manager – White Sands Missile Range Program (WSMR), 1995–1998
Managed all activities required for the engineering, network management system development, installation, testing, cutover, and acceptance of an enhanced network to manage, schedule, and transport data for mission operations at White Sands Missile Range.

Program Manager – Defense Logistics Agency Program (DLA), 1994–1995
Managed all activities required for the engineering, installation, testing, cutover, and acceptance of a 20,000-line COTS ISDN digital central office telephone system. Activities included inside plant, outside plant, site preparation, network management system, switch installation, database, Enhanced 9-1-1, Commanders Conference, and the establishment of a 10-year logistics return and repair support.

Project Manager, 1992–1994
Project Manager for the Carlisle Barracks Site of the Major Command Telephone Modernization Program (MTMP). Managed all activities required for the engineering, installation, testing, cutover, and acceptance of a 5500-line COTS ISDN DCO with three remotes.

Production Manager, 1990–1992
Managed a 60+ person, multi-shift, vertically integrated electromechanical assembly organization consisting of five separate departments. Responsible for budget and schedule compliance, staffing and training, maintaining and improving departmental utilization, productivity and quality goals.

EDUCATION

Northeastern University, High Technology MBA Program, MBA, 1988

University of Vermont, BSEE, 1984

Defense Systems Management College Program Manager's School, Fort Belvoir, Virginia, 1995

PROJECT MANAGER – PAUL C. CHOTKOWSKI

Mr. Chotkowski is a results-oriented PMI-certified Program Manager with more than 32 years of Program Management, Project Management, general management, technical support, business process development, operations management, new business development, outsourcing and foundation services development, pricing and bids/proposal support, and sales support experience in the communications industry. Program management experience in both North America and International/ Expatriate experience in Asia and Europe both in commercial and government sectors.

CAREER SUMMARY

General Dynamics Information Technology, Needham, Massachusetts

Operations Manager Systems Integration, Jan 2008–Present

As Systems Integration (SI) Operations Manager, reported directly to Vice President of Unified Communications. Oversee project and site manager's requirements including site orders, assets, program reporting and scheduling, financial management, and promoting compliance with Quality, Environmental, Health and Safety programs, and Records Management policies, as well as, other General Dynamics policies and procedures. Responsible for overseeing the successful implementation of over 100 projects valued at $250M as Operations Manager.

- Ensures customer satisfaction for both internal and external customers.
- Schedule and plan project/site resources accordingly.
- Monitor and coordinate all aspects of the SI organization.
- Issue a program plan, detailing how all aspects of the program will be controlled and implemented.
- Support Project Management Office awareness and understanding of plans for the administration of the SI organization.
- Support contractual items are accomplished / delivered in accordance with the contract.
- Enforce risk management methodology and subsequent implementation of corrective action plans, as required.
- Manage the contract change process.
- Personally managed the following projects:
  - U.S. Air Force Air Education and Training and Training Command – Operator Consolidation – Consolidation of Operator Services and Alarm Monitoring of 15 Air Force Bases to central location in San Antonio.
  - Air Force Network Operations Help Desk Call Center – Deployed four global call centers for Air Force Help Desk supporting 800 Agents and 90,000 users.
  - Defense Information Systems Agency (DISA) Enterprise Service Center – Managed the engineering, furnishing, installation, commissioning and testing of a Unified Communications Solution supporting 120,000 users.
  - U.S. Air Force – Air National Guard First Response – Managed team deploying E9-1-1 systems to over 40 bases worldwide.

Project Manager – U.S. Air Force In Europe (USAFE), Jun 2003–Jan 2008

As the USAFE Project Manager, was responsible for all coordination necessary to manage all aspects of the individual tasks assigned in the European theater. Responsibilities include: Schedule and financial management; ensuring the overall success of all upgrade projects, Estimate at Completion (EAC) responsibility, providing up-to-date site configurations, coordinating engineering support and management of subcontractors to assure compliance with the requirements of a Delivery Order including Contract Data Requirements Line items. As Project Manager, had responsibility for project schedules and financial goals for over $45 million in contract awards.

Darwin Partners, Wakefield, Massachusetts

Program Manager – Consultant, Nov 2002–Jun 2003

Provide consulting services on behalf of Darwin Partners to various communication clients including AT&T Wireless and MLC Wireless. Developed and delivered a Program Management Office (PMO) handbook for use by the client's project managers in assisting them in structuring and formalizing their project offices. Develop Project Management Plans (PMP), communication plans, quality management processes as well as perform analysis on client's project management processes and procedures. Develop statement of work documents for a client's national program.

Nortel Networks Corporation Scotland, Ireland, Hungary

Senior Program Manager, May 2001–Jun 2002

Program managed a $45 million LAN upgrade program for a major contract manufacturer's European sites in Scotland, Ireland, and Hungary.

Nortel Networks Corporation, Westborough, Massachusetts

Senior Program Manager, Jan 2001–Apr 2001

Nortel Networks Corporation Richardson, Texas

Senior Program Manager, Nov 1999–Dec 2000

Program managed two multi-million dollar CLEC installations and one optical deployment in South Carolina, Connecticut, and Rhode Island. Maintained project schedules, negotiated subcontractor agreements and supplier agreements and change control processes.

Nortel Networks Corporation, Richardson, Texas

Senior Manager /Proposals & Pricing, Nov 1997–Nov 1999

Lead the pricing and approval process for Satellite Network Solutions (SNS) as Bid Manager. Developed cost and pricing analysis for potential programs. Managed a centralized proposal response team supporting offices in Texas, Maryland, Canada and the UK.

Developed Statements of Work, Program Plans using Microsoft Project, Budgets, Risk Identification, and assisted in Staff Acquisitions. Provided pricing and responses, performed due diligence and conducted on-site bid support to customers for programs located in Asia, Europe, and North America.

Northern Telecom Inc., Richardson, Texas

Senior Staff Manager /Program Manager, Jan 1995— Oct 1997

As a member of the sales and marketing team for Mobile Satellite Systems, matrix managed a proposal team to respond to a Mobile Satellite System bid for a 17-year program with global locations with a value of one billion dollars.

Senior Staff Program Manager, Apr 1992— Dec 1994

Contracted to develop, direct and manage a state-of-the-art telecommunications organization for a new start-up joint venture between two major telecommunication equipment suppliers. Company consisted of 1000 employees at 16 locations in 7 countries. Responsibilities included the development of tactical and strategic plans for both voice and data communications for each location. Responsible for budget planning as well as the telecommunications budget of over $20 million dollars.

Senior Manager, Network Integration, Oct 1990— Mar 1992

Northern Telecom Inc., South Korea

Senior Technical Support Engineer, Oct 1988–Sep 1990

Provide Emergency Technical Support Services out of the Depot Level Software Support Center (DLSS) to the U.S. Army in Korea.

Project Manager, Aug 1986— Sep 1988
Established a Northern Telecom presence in Taegu, South Korea. Responsible for the cutover and maintenance of 8 MSL-100s and one Tandem NonStop II computer. Created routing and database loads for 20 switches in the country.

Northern Telecom Inc. Framingham, Massachusetts

Technical Support Engineer, Aug 1984— Jul 1986
Provided on-site support for maintenance, translations and consultation for an MSL-100 and 6 SL-1 sites.

Systems Design Engineer, Oct 1983— Jul 1984
Responsible for the design and cutover of Meridian SL-1 systems in the region. Specialized in hospital, hotel, university and financial institution applications.

SECURITY CLEARANCE

Secret – Updated: Disco 6/6/11

CERTIFICATION

Program Management Professional – PMP – Program Management Institute, June 2001

EDUCATION

Boston College, Chestnut Hill, Massachusetts

Bachelor of Science, 1982, Computer Science, Business Administration

CONTRACT MANAGER – STEPHEN L. WOODWORTH

Mr. Woodworth is a contracts management professional with more than twenty years' experience working in partnership with senior leadership managing, negotiating, and drafting complex contractual arrangements for commercial and government customers. Demonstrated ability to manage multiple projects, establishes priorities, and complete tasks in a timely manner to achieve goals. Proven knowledge to identify and resolve business and contract law issues. Strong attention to detail, excellent writing and drafting abilities, and exceptional customer focus skills. Capable of working as a team member or independently on complex tasks, and in accordance with established policy and procedures.

CAREER SUMMARY

General Dynamics Information Technology, Inc., Needham, MA
General Dynamics delivers superior IT services and solutions to military, government, and commercial customers worldwide

Contracts Manager, Defense Solutions Division, IT Services, Sep 09–present

- Responsible for contract management functions, including drafting and negotiating prime and sub-tier contracts for government and commercial contracts, in accordance with applicable contract rules and regulations.
- Serve as subject matter expert and member of program team, leading/supporting negotiation team and provide contract expertise to develop and negotiate creative solutions in support of new and follow-on business.
- Review government solicitations to identify government needs, proposal instructions and evaluation criteria and communicates the same to leadership and proposal team. Participate in proposal preparation, review of the SOW, T's & C's, reps and certs and cost estimates. Performs risk assessment including Organizational Conflict of Interest (OCI) and contract type. Obtains management approval/sign off to submit proposal in accordance with delegated authority.
- Draft and negotiate Non-Disclosure Agreements (NDAs), Subcontract Agreements, Teaming Agreements, PSAs and other agreements as required.
- Responsible for completing CPARS, DD254, research EDA for agreements/mods, performing Visual Compliance on contractors and individuals as part of corporate policy and government subcontracting requirements.
- Responsible for developing solutions to problems, partnering with program team and ensuring proper flow down and compliance with contract T's and C's ensuring execution is consistent with company objectives.
- Act as the focal point with the government for all contractual matters and the liaison with customers and internal departments for all matters affecting contracts.
- Compile and analyze data, and maintain current contracts, files and records. Draft and control formal correspondence with the government Contracting Office. Monitor and ensure compliance with contract terms, special provisions, warranties, deliverables and funding requirements. Administer ITAR/EAR requirements.
- Attend program reviews/kick-off meetings at government sites to identify potential contract changes, including Engineering Change Proposal (ECP), Request for Equitable Adjustment (REA), and Change Control Process (CCP).
- Issue sub-tier POs via Enterprise Spend Management (ESM) / Ariba system, enter contract terms into Oracle and the VPO.

Contracts Manager, NY Statewide Wireless Network Program, General Dynamics Wireless Services, Jan 06–Aug 09

- Worked directly at the customer site acting as the focal point with customer and liaison with internal departments for all contractual matters for this $183M award.
- Responsible for developing solutions to problems, partnering with Program Team and ensuring proper flow down and compliance with all contract terms and conditions.
- Establish terms and conditions of contracts and subcontracts ensuring compliance with legal and company requirements. Created, maintained and distributed all required forms for use by the program team.
- Managed and participated in the development of the change order process, including creating forms, policies, and procedures, ensuring no Out of Scope (OOS) work performed without contractual funding.
- Liaison and SME with the DOL and the State of New York with respect to wage determination requirements.
- Participated as part of a corporate team with respect to managing a REA and Termination for Convenience.

Sr. Contracts Specialist, General Dynamics Wireless Services, Jul 03–Jan 06

- Responsible for contract management functions, including drafting, negotiating and administering prime and sub-tier contracts for commercial and local government contracts, in accordance with applicable contract rules and regulations.
- Member of a program team to review customer solicitations to identify customer needs, proposal instructions, risks, review SOW, terms and conditions, reps and certs. Obtain final management approval to submit proposal per delegated authority.

Contracts Manager, Pegasystems, Inc., Cambridge, MA, Jul 01–Jul 03

- Responsible for contract management, negotiation, drafting and administration for all commercial contractual arrangements in accordance with corporate guidelines and contract rules and regulations. Managed the installation of Pegasystems first contract management database and responsible for maintaining all original contract files and correspondence.
- Acted as the focal point of contact with customer and internal departments for all matters affecting contracts, reporting directly to General Counsel.

Contracts Specialist, Netscout Systems, Inc., Westford, MA, Nov 00–Jun 01

- Draft, review, revise and negotiate contracts including but not limited to software license agreement, PSAs, vendor contracts, reseller, distributor, development, change orders, amendments, and non-disclosure agreements. Prepare metrics on contract operations for reporting to management. Created and instituted use of standardized department forms and procedures.
- Obtain appropriate internal approvals for contract terms and provisions. Appropriately escalate legal and factual issues to General Counsel and assist in their resolution.

Contracts Specialist Harte-Hanks Data Technologies, Inc., Billerica, MA, Jun 99–Nov 00

- Review, negotiate and draft all supplier/vendor agreements, building service contracts, equipment leases, and consultant relationships for this $2 billion dollar division.
- Managed daily activities and correspondence surrounding all aspects of vendor relationships.
- Developed and instituted, internal policies, forms and procedures, resulting in more timely responses to vendor agreements, along with obtaining most favorable pricing.

Sr. Contracts Consultant Banyan Systems Incorporated, Westboro, MA, 1994–1999

- Participate in all phases of software license negotiation and administration with direct customers, resellers and distribution partners, while interfacing with the sales force, senior management, finance and administration.

- Particular detail provided to protect intellectual property rights and adequate limitation of liability.
- Review, negotiate and digest real estate leases and negotiate lease disposition agreements.
- Train and mentor contract administrators and support staff.

Contracts Manager, World Wide Sales, 1988–1994

- Managed, negotiated and administered software licenses, reseller, consulting, maintenance and nondisclosure agreements, with strong emphasis on protecting the intellectual property of Banyan and third-party products.
- Traveled to domestic customer and prospect locations to negotiate contractual agreements.
- Researched contractual language as a result of customer and internal inquiries, resulting in the resolution of discrepancies and drafting contract amendments, correspondence, default notices and settlement agreements.
- Developed and instituted policies, procedures, filing systems, and standardized agreements/forms for this start-up contracts administration department. Train and supervise contract administrators.

EDUCATION

Bentley University, Waltham, Massachusetts – Awarded Comprehensive Paralegal Certificate, ABA approved program

University of Maine at Farmington – Bachelor of Science, Special Education

Professional Licensure: Notary Public, Real Estate Sales License, Paralegal Certificate

Skills: MS Word, Excel, PowerPoint, ESM/Ariba, Markview, Oracle, VPO/Project Vista, CPARS, EDA, Visual Compliance

TRANSITION/MIGRATION LIAISON – GLENN ROACH

Mr. Roach is an accomplished and knowledgeable Emergency Communications Professional with more than 28 years of operations and administrative experience in government, corporate and entrepreneurial emergency communications settings. He is a Certified Emergency Number Professional (ENP). His areas of expertise include 9-1-1 and public safety communications planning, administration, operations, technology, regulations and legislation at the international, federal, state, and local level. In addition, Mr. Roach has 20 plus years of operational and technical expertise to include network, selective routing, ANI, ALI database (Stand-Alone ALI (SALI) and legacy) wireless, wireline, VoIP, peripheral equipment, and applications in both traditional and non-traditional environments. Also, he has 20 plus years of experience in public safety emerging technologies and Next Generation Services (NG9-1-1). Mr. Roach has 30 plus years of experience in drafting and administering standard operating procedures for telecommunications, call centers, and public safety communications. He has over 20 years of experience with various public safety communications equipment and systems Mr. Roach also has played a major role on public safety communications related standards setting bodies to include NENA, ESIF, and ATTIS, and has recently been involved in the National Public Safety Broadband effort with FirstNet He also has many years of experience in legislative and regulatory processes to include drafting and writing legislation and regulations.

CAREER SUMMARY

Winbourne Consulting, LLC

Vice President 2010–present

Public safety emergency communications consulting and program management. Subject matter expert in emergency communications planning, operations, administration, technology and regulations.

- US Trade and Development Agency (USTDA) – India Integrated Emergency Communications System (IECS) Feasibility Study – Technical Project Manager/SME
- US Trade and Development Agency (USTDA) – Ukraine National Emergency
- Telephone Call Response System (112) Feasibility Study – Project Manager
- Charlotte Mecklenburg, North Carolina Police Department Command Center Redesign Project – Emergency Communications SME
- Washington Metro Transit Authority Police Department CAD/RMS Replacement Project – 9-1-1 SME
- City of Albany/Dougherty County, Georgia Criminal Justice Information Systems RFP Project – 9-1-1 SME
- Arapahoe County Colorado 9-1-1 Authority – 9-1-1 Strategic Plan Gap Analysis – Project Manager/SME
- Metropolitan Washington Council of Governments – Assessment of 9-1-1 Outage related to Derecho Storm on June 29, 2012 – SME/Report Author
- Commonwealth of Virginia – Secure Commonwealth Panel – 9-1-1 Sub Panel – Assisted in the assessment and provided subject matter expertise on the state of 9-1-1 service in Virginia – 9-1-1 SME
- Modernization of the Haiti National Call Center Project – United Nations Development Program (UNDP) – Performed an assessment and provided subject matter expertise on the current condition of emergency call reported systems for the Country of Haiti. - 9-1-1 SME
- US Department of Homeland Security (DHS) Office of Emergency Communications (OEC) Interoperable Communications NG9-1-1 Technical Assistance Program – NG9-1-1 Consultant/SME

Emergency Public Safety Communications, LLC

Owner/CEO, 2010–2012

Public safety emergency communications consulting and program management. Subject matter expert in emergency communications planning, operations, administration, technology and regulations.

- State of Hawaii Wireless Enhanced 911 Board, Independent contractor providing executive director program management services to direct the day-to-day business for the state agency responsible for planning, implementation and administration of wireless 9-1-1 services – Executive Director

Intrado Inc., Longmont, CO, 2003–2009

Director, Consulting and Systems Integration, 2007–2009

Led the consulting and implementation group for world's largest 9-1-1 operations systems company. Responded to leads and Requests for Proposals (RFPs), and cultivate existing customer accounts. Guided customer system assessments and execution of customized solutions. Mr. Roach also held positions with Intrado to include Director of product Development and Director of Sales Engineering.

Telecommunication Systems Inc. (TCS), Seattle, WA

Vice President 9-1-1 Services, Director 9-1-1 Services, Director of Public Safety, 1998–2003

Directed daily operations of wireless 9-1-1 services, including business and product development. Maintained productive relationships with federal, state and local public safety authorities. Monitored and influenced legislative and regulatory issues involving emergency communications.

Capital Area Planning Council, Austin, TX

Emergency Services Director, 1995–1998

Administered 9-1-1 services for 10-county region surrounding Austin.

Commonwealth of Massachusetts, Burlington, MA

Executive Director, Statewide Emergency Telecommunications Board, 1992–1995

Directed the day-to-day Board business for the state agency responsible for planning,

implementation and administration of the state 9-1-1. Won acceptance from state and local officials to introduce fees supporting emergency communications. Launched 9-1-1 services statewide to 270 Public Safety Answering Points fees, resulting in 100% state coverage. Ensured success of program through thorough training of planning council implementers.

9-1-1 Coordinator for the State of Texas, 1990–1992

9-1-1 Supervisor for the City of Houston, 1988–1990

EDUCATION

Psychology & Sociology, San Jacinto Community College, Friendswood, TX

Math & Science, Alvin Community College, Alvin, TX

PROFESSIONAL ORGANIZATIONS

- **The National Public Safety Telecommunications Council (NPSTC) – LTE Console Working Group, 2013–present**
- **Federal Communications Commission** – Communications Security, Reliability, and Interoperability Council (CSRIC IV) – Working Group, 2013–present
- Associated Public Safety Communications Officers (APCO), 1986–present
  - 911 Emerging Technologies Committee, 2010–2013
- National Emergency Number Association (NENA), 1986 – present
  - NG9-1-1 ICE Steering Committee, 2011–2013
  - Technical Standards Committee, 1999
  - Wireless Committee ,1999
  - Accessibility Committee, 1991–1998
  - National Issues Committee, 1994–1995
  - Staffing Committee, 1994–1995

  - International Committee, 1992–1995
- National Association of State Nine-One-One Administrators, 1992–1995, 2009–2011
- E9-1-1 Institute, 2005–present, Board of Directors, 2010–2011
- Industry Council for Emergency Response Technologies (iCERT)

SYSTEM ARCHITECT – PAUL BRILLAUD

Mr. Brillaud has 23 years of success delivering technology solutions to government and enterprise markets, articulating strategic technology vision, and building business efficiency for emerging technology products and services.

- Exceptional technical depth in converged IP services (voice, video, data), including Cloud services, infrastructure, UC, NG9-1-1 operations support, and cyber security.
- Providing team lead for program, architectural, and implementation engineering to achieve business and technical performance and program success.

CAREER SUMMARY

General Dynamics Information Technology, Needham, Massachusetts

Lead Solutions Architect – Unified Communications, Mar 2010–Present

Provide technical leadership for pre-sales and post-sales technology engagements across all IP converged services for federal, state, and enterprise markets. Lead solution development, including partner management, proposals, technology validation, and implementation. Drive successful technology solutions to market, with program level responsibilities, including technical performance, schedule compliance, and reporting and action resolution.

- Served as chief architect for NG9-1-1 solution development, including engagement with partners for functional performance and compliance, customer interactions and implementation. Managed NG9-1-1 testing lab.
- Chief Architect for national FAA voice network modernization to UC (private cloud) supporting. Lead engineering activities from architecture to solution implementation, turn-up, and testing, including Network and Security Operations Center. Provide program-level reporting and visibility.

MetaSwitch, Enfield, UK

Sr. Director Solution Sales & Consultation, Feb 2008–Oct 2009

Lead Sales and Solutions consulting for converged IP voice and UC solutions to systems integrator, state/local and large enterprise verticals, including voice switching, mobility and applications. Managed team nationally, drove industry recognition and public vision.

Cedar Point Communications, Derry, NH

VP Sales & Offer Management, New Markets, Apr 2005–Feb 2008

Senior leader responsible for building ground-start entry into tier 2/3 CLEC and large enterprise verticals for IP switching and network convergence. Lead solutions engineering and sales for voice systems and unified communication. Manage partner strategies and project implementations.

Integral Access, Inc., Chelmsford, MA

Sales Consulting Director, Mar 2003–Dec 2005

Drive technology solutions for multi-protocol access gateway and Broadband-DLC. Identified and managed partners. Provided technical vision for voice over Digital Subscriber Line Access Multiplexers (DSLAM).

Wavesplitter Technologies, Freemont, CA

Regional Vice President of Product Marketing, Nov 1999–Dec 2002

Lead East Coast and Canadian solutions consulting and sales for optical subsystems, components, and modules to carrier and OEM verticals, for optical transport, including Reconfigurable Optical Add-Drop Multiplexers (ROADMs), xWDM, and signal conditioning.

Lucent Technologies, N. Andover, MA

Product Management Director, Optical Infrastructure, Jan 1992–Nov 1999

Lead team technical and business staff in definition and delivery of evolving high-capacity long haul and access loop optical solutions including SONET, PN, xWDM- and metroethernet.

AT&T Network Systems, Andover, MA

Product Manager, Optical Networks, Jun 1988–Jan 1992

Managed definition and evolution of SONET OC3/12/48 product conceptualization, development, and market introduction. Lead commercialization to Tier 1 carrier markets.

EDUCATION

Boston University, Boston, MA – Master of Business Administration, Finance

Northeastern University, Boston, MA – Bachelor of Science, Mechanical Engineering

IMPLEMENTATION MANAGER – JEFF MODICA

Mr. Modica has 17+ years of Engineering and Project Management experience deploying telecommunication systems for the Department of Defense. He is a Senior Technical Project Leader whose superior understanding of voice switching technologies and customer requirements has led to successful project implementation of Department of Defense programs.

- Experience managing multiple complex voice infrastructure deployments with a focus on business awareness and schedule performance
- Practical knowledge of customer vision and associated voice enterprise requirements
- Excellent teamwork, customer service, and interpersonal and communication skills
- Solution-focused implementation experience deploying medium and large-scale enterprise voice system engineering projects
- 15+ years of design and implementation experience with an emphasis on best practices and business process

CAREER SUMMARY

General Dynamics Information Technology, Needham, Massachusetts

Senior Project Manager/Lead Engineer, 1995–Present

- Senior Project Manager/Lead Engineer for USMC and Navy Voice Upgrades to include both legacy Nortel and Avaya upgrades.
- Successfully performed as Project Manager for Navy, Army, and Marine Corps voice switch modernizations, upgrades, and replacements. Recent successful implementations include:
  - At Navy Bases at Pensacola, Corey Station, Saufley Field, Oceana, Dam Neck, Newport, and Yorktown was Overall Project Manager for EFIT&C Avaya-based Communication Manager 6.0 systems
  - Lead Project Engineer for DWDM and Telecommunications Upgrades for the USMC in Okinawa and Camp Fuji, Japan
  - At MCLB Barstow, Overall Project Manager for the Telecommunications Upgrade
  - At USMC Camp Lejeune, Overall Project Manager for the Remote Switch Installations at Hadnot Point and Camp Johnson
  - At Naval Station Everett, EFIT&C a new Avaya-based Communication Manager 4.0 solution, replacing an existing legacy Nortel system.
  - At NAS Sigonella, upgraded the Nortel SL-100 Multi-Function Switch (MFS) hardware and software from XA-Core with software SE06 to SE09.1.
  - EFIT&C an Avaya-based Communication Manager 4.0 solution consisting of dual Avaya S8720 Servers, Avaya G650 Gateways, Extreme x450-24p Ethernet switches, and new 1500VA Uninterruptible Power Systems (UPS) at Naval Auxiliary Landing Field (NALF), San Clemente Island, CA
  - Naval Weapons Station Earle, Colts Neck, NJ; and Naval Hospital Bremerton, Bremerton, WA
- Performed as implementation operations lead during multiple simultaneous site deployments within a specific program.
- Ensures projects operations are completed on time, on budget, and with minimal site operation disruptions.
- Prepares project plans, sets project goals and deadlines.
- Leads and directs others supporting organizations, measures and evaluates performance, works with the customer community to coordinate deployment activities.

- Provides status summaries of project performance to senior program management and ensures project tasks are completed on time and to the satisfaction of the customer. Responsible for timely procurement and delivery of material.
- Responsible for system engineering design, documentation development, Type Accreditation, implementation, and site cutover to include hardware recommendations, deployment approach, cutover and submission of the program deliverables.
- Led team working group meetings with customers, subcontractors, and local base resources to ensure continuous communication between design team, implementation team, and the customer.
- Performed as enterprise voice switching engineering lead for major Navy and Army proposal development cycles. Recommended equipment selection based on design requirements and best customer value.
- Performed as Sr. Project Manager for several DSN voice switch modernizations, including:
  - NAS Sigonella (2009-2010) – Upgraded the Nortel SL-100 Multi-Function Switch (MFS) hardware and software from XA-Core with software SE06 to SE09.1
  - Naval Auxiliary Landing Field (NALF), San Clemente Island, CA (2008–2009) – Upgrade of Avaya Small End Office (SMEO) to CM 4.0
  - Naval Weapons Station Earle, Colts Neck, NJ (2008–2009) – Upgrade of Avaya SMEO to CM 4.0
  - Naval Hospital Bremerton, Bremerton, WA (2008–2009) – Upgrade of Avaya SMEO to CM 4.0
  - NAS Jacksonville (2007–2009) – Modernization Upgrade of Lucent 5ESS
  - Fort Carson, CO (2006–2007) – Technical Design for Nortel CS 2100 Split Core, 3 MG9Ks, and 1 CS 1000M
  - Fort Sam Houston (2005–2006) – Physical relocation of an Remote Switching Center (RSC)
  - Picatinny Arsenal, NJ (2002–2003) – Replaced a GTD-5 with Meridian 1 Option 81C
  - Fort Lee, VA (2002–2003) – Replaced 7 Mytel PBXs with 1 Nortel SL-100 and 5 remotes

EDUCATION

University of Massachusetts, Amherst, BBA in Finance and Economics, 1995

Several Nortel Networks Workshops

OPERATIONS MANAGER – THEODORE GAUSMANN

CAREER SUMMARY

General Dynamics Information Technology

Senior Operations Manager, 2013–Present

Manager of 24x7x365 Network Operations Center (NOC) providing technical support services to field technicians and end users. Technologies supported include voice switching systems and related equipment and networks, enterprise VoIP systems, and E9-1-1 systems. Manages technical support staff providing global support to the United States Air Force, the Federal Aviation Administration (FAA), and state and local governments. Uses Remedy trouble ticketing system to track and manage all incidents. Coordinates escalation to Original Equipment Manufacturers (OEMs) when additional support is required, and dispatches technicians and engineers to sites to resolve issues that cannot be addressed remotely.

Business Operations Manager, 2010–2013

Led business operations organization of $200 million program office responsible for design and installation of IT infrastructure along with Audio-Visual (AV) and wireless systems for the new DoD Mark Center buildings, including the relocation of over 6,000 customer tenants. Coordinated and reviewed all proposal estimating/writing/pricing activities and conducted formal management reviews. Coordinated the review, preparation, and delivery of over 1,000 formal contract reports and documents. Supervised the contract quality assurance and logistics functions, and managed the program security, IT support, facilities management, and site administration activities.

Program Director, 2006–2010

Head of customer-focused business area with responsibility for contract performance and customer satisfaction on U.S. and global programs supporting the Defense Information Systems Agency (DISA). Successfully managed transition project that relocated global 24x7 network monitoring function from two OCONUS sites in Germany and Hawaii to Illinois (Scott AFB). Programs involved telecommunications network management, maintenance, and engineering support; system administration; and other operations and maintenance. Ensured customer satisfaction by successfully managing contracts' technical, cost, and schedule performance.

Program Manager, 1998–2006

Head of program office managing over 100 field service employees and subcontractors at U.S. and overseas sites. Responsible for four different technical services contracts totaling $10 million in annual revenue. Programs supporting Department of Defense and Department of Energy involved telecommunications operations and maintenance, network management, and engineering support; LAN management, system administration, 24x7 help desk support, and LAN/MAN maintenance; telecommunications network operations and maintenance; multi-site fielding (design and deployment) of inside plant and outside plant cabling and telecommunications hardware.

EDUCATION

Bachelor of Business Administration – Finance, University of Wisconsin-Eau Claire, Eau Claire, WI

DIRECTOR, ENGINEERING AND TECHNOLOGY – PETER JOO

Mr. Joo has over 36 years of combined solid telecommunications technology experience. 20 years of military telephone system operations and maintenance and voice system technology updates and migration planning and implementation. Served as voice systems technology advisor to the United States Air Force's largest Major Command, consisting of 22 large USAF bases. Over 16 years of telecommunication system Project Management and voice system engineering experience with General Dynamics. Led system engineering and project management for the DoD's largest voice network establishment and transition for the Defense Information Systems Agency (DISA), resulted in totally successful on-time and on-budget migration of over 2,000 T-1 trunks and 600 large telephone switching systems to the new voice network.

CAREER SUMMARY

General Dynamics Information Technology, Needham, Massachusetts

Director, Engineering and Technology, 2007–present

Led an engineering team developing USAF's E9-1-1 system design, specification and deployment case analysis. Developed engineering specifications, deployment guide, and Total Cost of Ownership (TCO) analysis for stand-alone PSAP, hosted, regional, and pilot system systems. Our documents became USAF's standards for USAF wide deployment of E9-1-1 systems. Led engineering and deployment of over 75 E9-1-1 PSAP systems for the USAF.

Led the engineering effort for the USAF Enterprise Voice Consolidation System (EVCS). The EVCS system establishes regionalized network management, situational awareness, and consolidated O&M capability for nearly 900 voice systems worldwide for the entire USAF.

Led the engineering, deployment, and program management for the DISA's Defense Switched Network (DSN). Orchestrated the engineering and managed the entire program which involved installation and cutting over the entire DoD's voice network. This $34M project consisted of installing six carrier-grade telephone switching systems with thousands of trunks to 600 telephone switching systems and 1,700 T-1 circuits supporting 230,000 users.

Led development of enterprise solution for the Air Force Network Operations Enterprise ACD system, supporting over 850,000 customers worldwide. Selected as the best solution and implemented the solution on-time, on-budget.

Led engineering and deployment of DoD's new worldwide Unified Communications (UC) infrastructure at 19 locations. The enterprise UC architecture consists of DoD-certified WAN Soft Switches and security boundary systems.

Led the engineering organization for developing SIP-based voice network solution for the entire Federal Aviation Administration (FAA). The enterprise voice systems serves over 900 FAA locations in continental US.

Program Manager, 2003–2006

Responsible for overall program management of $435M Worldwide Integrated Digital Telecommunication System (WIDTS) program, ensuring optimal technical solutions are engineered and successful implementation of all projects on time and on budget.

Maintained consistent high customers (A+) satisfaction level with the USAF, DISA, and Navy customers under the WIDTS program.

Provided system consulting to USAF, Navy, and DISA customers on telecommunications system technology updates and expansion planning and system requirement definition.

Project Manager, 1997–2003
As the lead Project Manager and also as the voice system Subject Matter Expert (SME), developed nearly 1,000 voice system solutions and successfully managed well over 100 voice system projects, totaling over $100M in value.

Developed integrated solutions and deployed SONET, PBX, and voice subsystems, such as conferencing, ACD, billing, E9-1-1 systems, and DC and AC power systems.

Superintendent, Telephone Systems (HQ Air Combat Command, USAF), 1994–1997
Technical advisor on various OEM switching systems, and managed telephone system sustainment, technology upgrade planning and requirement development, budget, and implementation for 22 major USAF military installations.

Spearheaded a feasibility study on "Switchboard Regionalization and Outsourcing" for 18 Air Force bases in CONUS – a comprehensive study resulted in being the benchmark for other Commands in USAF.

Awarded the Command's Outstanding Manager of the Year Award for 1996

Telecommunication Systems Manager (USAF), 1977–1994
Managed variety of analog and electronic telephone switching systems and Nortel DMS-100 digital switching systems located throughout the AF.

Awarded 1992 Outstanding Telephone Switching Center of the Year, Pacific Theater 1992 Outstanding Communications-Electronics Maintenance Manager of the Year Award, and 1991 Outstanding Manager of the Year Award.

EDUCATION

Systems Management Courses for M.S., Florida Institute of Technology, FL

Bachelor of Science, Computer Science, University of Maryland, MD

Member National Emergency Number Association (NENA)

SECURITY CLEARANCE

DoD Top Secret Clearance

QUALITY MANAGER – CAROL C. KILCOURSE

CAREER SUMMARY

General Dynamics Information Technology, Needham, Massachusetts

Project Control Manager, 2008–present
Lead for internal/external ISO 9001 audits in Needham and remote sites. Develops relationships with Contracts, Finance, Business Development, and Program Offices to educate and document policy and procedures changes effectively. Educates over 800 employees on GDIT Quality Management System (QMS) procedures. Supports identifying, changing, and improving processes to meet our customer's needs as well as corporate requirements more efficiently.

Project Manager for WIDTS Program, 1997–2008
Managed installation of multiple SL-100/Meridian switches upgrades at various Air Force sites throughout the world. Coordinated and managed the Y2K upgrades for 76 Air Force sites. Managed the installation, testing, and deployment of two containerized SL-100 switches for emergency deployment anywhere in the world for the DoD. Managed installation and testing of battery plants/monitoring systems, ACD, and voice mail systems throughout USAF sites.

Program Coordinator, GTE Government Systems, 1995–1997
Coordinated the financial, program office, and contractual requirements for the Worldwide Integrated Digital Telecommunications Systems (WIDTS) program. Developed schedules, maintained milestone databases. Managed overall program requirements for 10-person Program Management Office (PMO).

EDUCATION

B.S. – Business Administration, Nichols College

Masters Certificate in Project Management, George Washington University

CERTIFICATIONS / LICENSES / TRAINING

PMP Certification, 2005–present

Office Locations of the GDIT Massachusetts Next Generation 9-1-1 Project

The location of the offices from which the work will be managed and the number of staff employed at each office:

Table 38. GDIT Office Locations for MA NG9-1-1 Project

Office Location	Type of Work	Staff Count
Needham, MA	Program Office Engineering i3 Solutions Interoperability Lab Staging and Testing Help Desk Network Security and Operations Center (NSOC)	800
Fairview Heights, Il	Backup Help Desk and Network Operations Center (NOC)	20
Herndon, VA	Security Operations Center (SOC) Services	400

Project Schedule

A proposed project schedule, work plan and project management plan that demonstrates its understanding of the engagement and of the tasks that must be completed;

A high-level overview of the Integrated Project Schedule is included as Figure 68 in Section 8.9 (Project Management), and the detailed IMS is included in Appendix L. In addition, our detailed

approach to execute to this plan is included in Section 8.13 (Migration, Deployment, and Installation).

Staffing Plan

Staffing plan for ongoing operation, support, and maintenance of the system, including but not limited to, NOC, help desk, field service, data center, and administrative staff;

GDIT's approach to program management combined with our depth of experienced resources enables our team to place the right resources in the right performance areas at the right time to expeditiously implement the MA NG9-1-1 project, and then maintain consistent, continuous support services throughout contract performance. GDIT and our subcontractors currently have 90% of the staff with the requisite skill sets identified for this project, and will be 100% staffed and operational shortly after contract award.

We recognize that our success and growth hinge upon our ability to recruit and maintain the finest available talent, and to do so quickly. We employ dedicated local recruiters who are experienced in technical recruiting. We are better able to attract and retain the best talent because our benefits package is flexible, competitive, and structured to attract and maintain the types of technical employees the Commonwealth requires for MA NG9-1-1. Our tried-and-proven recruiting process enables us to fill openings quickly and effectively, and we use labor-saving tools such as ResumeWare to streamline recruiting functions and reduce interview/selection time. The cross-company use of tools such as ResumeWare promotes collaboration and sharing of existing personnel, prospective employees, and information resources.

Figure 99 represents the labor effort by month required to implement Milestones 1-4 and support services through 30 June 2016. Figure 100 represents the staffing plan for the ongoing operation, support, and maintenance of the system for 1 July 2016 through 3 August 2019.

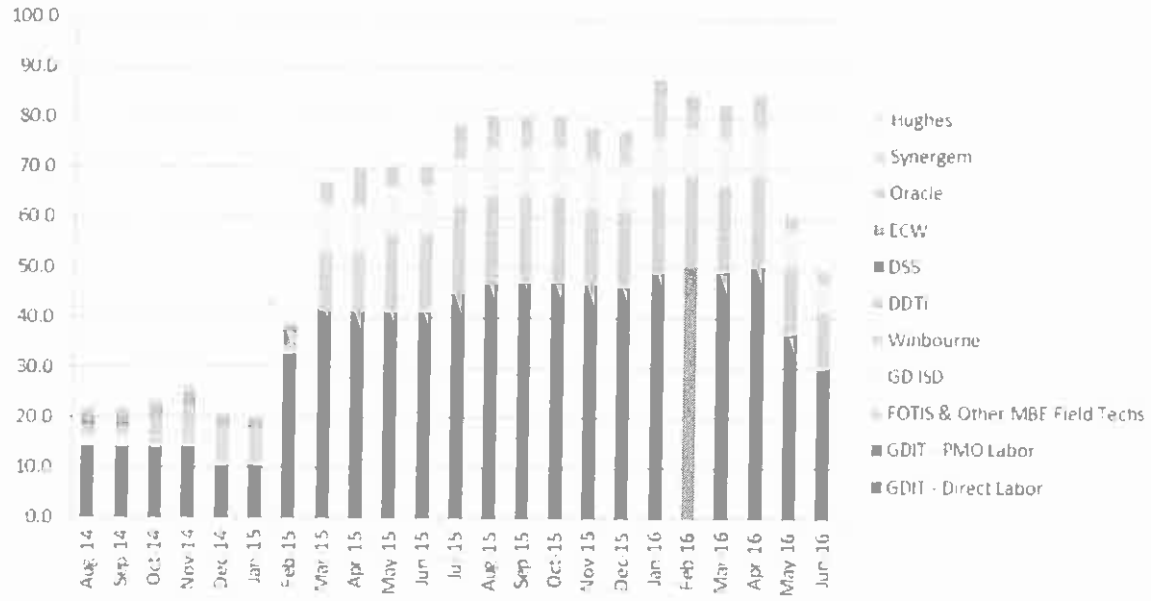


Figure 99. Milestones 1–4 and Support (Years 1–2) FTEs by Month

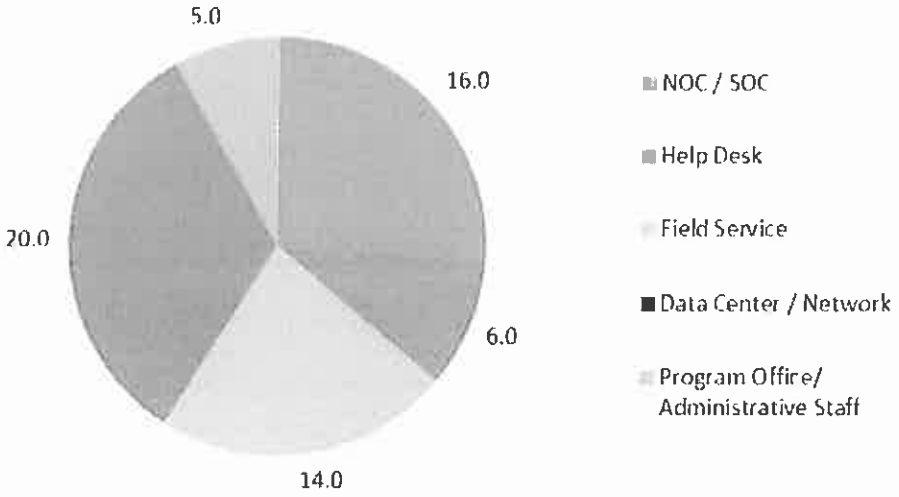


Figure 100. Staffing Plan for 1 July 2016 through 3 August 2019

Training Plan

Training Plan:

GDIT new hires, current employees, and subcontractors all have required learning requirements to fulfill at certain times. GDIT's Learning Management System, myLMS, provides a fully integrated web-based learning solution for professional development initiatives and myLMS contains the following functionality:

- Delivery and System of Record for GDIT Required Learning
- Delivery, Tracking and Transcript Records for E-learning courses from SkillSoft, GDIT's e-learning content vendor
- Enrollment, Tracking and Transcript Records for instructor-led courses offered by GDIT
- Enrollment and Tracking of Curriculums (associated courses)

Learning resources are available for GDIT employees seeking professional certifications or recertification. GDIT's e-learning content includes coursework in support of business, desktop and IT Professional certifications.

The LMS system and required coursework will be updated to include specific training requirements, regular interval updates, and industry standard skill set testing for the MA NG9-1-1 project.

9.1. OPEN RATINGS/DUN & BRADSTREET (D&B)

The Strategic Sourcing Team (SST) has chosen to utilize independent parties, Open Ratings and Dun and Bradstreet Information Services (D&B), to assist in the evaluation process in two areas, reference checking and financial stability. The required reports are the "Supplier Qualifier Report" and the "Past Performance Evaluation (Supplier Performance Review)." The "Supplier Analysis Report" may be substituted for the "Supplier Qualifier Report."

Bidders are urged to request the Open Ratings/Dun and Bradstreet reports as soon as possible. Typically, reports can be prepared within thirty (30) days, however, there can be delays in report preparation, so bidders ***should NOT wait*** *until thirty (30) days before the Solicitation is due to request the reports. In particular, delays can be lengthy if Open Ratings is unable to contact a sufficient number of a bidder's references to prepare a report, and must contact the Bidder for additional references. It is the bidder's responsibility to submit references that can be contacted readily.*

Bidders should note that Open Ratings will use the company's legal name when requesting surveys. If clients are more likely to recognize the company's "doing business as" name, it is up to the bidder to let their clients know they may be asked by Open Ratings to complete surveys referencing the company's legal name.

GDIT complies with the RFR specification. GDIT submitted our request for the "Supplier Qualifier Report" and the "Past Performance Evaluation (Supplier Performance Review)" to Open Ratings and Dun and Bradstreet Information Services (D&B) and received a copy of the reports sent to the Commonwealth in a timely manner.

9.1.1. How to Request Reports

It is recommended that all Bidders submit the request for the reports directly to Open Ratings via http://www.ppereports.com/. When placing an order for the Past Performance Evaluation (Supplier Performance Review) and the Supplier Qualifier Report, select the "State and County" report option at the appropriate prompt during the ordering process. The Bidder must pay online with Open Ratings for both reports.

Bidders must request that a copy of each report be sent to Karen Robitaille, State 911 Department, 1380 Bay Street, Taunton, MA 02780 Tel 508-821-7221, Fax 508-828-2585, Karen.Robitaille@state.ma.us. A copy will also be sent to the Bidder's contact person named on the request form in the recipient section.

Bidders should note that it is not acceptable for the Bidder to simply include the reports in their proposal or to email the reports themselves, only reports emailed by Open Ratings and/or Dun and Bradstreet to Karen.Robitaille@state.ma.us will be acceptable.

Bidders must ensure that the company name given on the Open Ratings/Dun and Bradstreet reports matches the name on the Bidder's Response. Reports for parent companies or subsidiary companies are not acceptable.

GDIT complies with the RFR specification.

9.1.2. Use of Reports Obtained Previously

If bidders have had the required reports completed by Open Ratings and/or Dun and Bradstreet within six months of the release date of the RFR, those reports may be submitted in lieu of obtaining new reports. However, the bidder must arrange for Open Ratings and/or Dun and Bradstreet to email copies of the reports directly to Karen.Robitaille@state.ma.us. Again, reports will not be accepted if they are simply included in the bidder's Response or emailed by the bidder.

GDIT complies with the RFR specification. GDIT did not have the required reports completed by Open Ratings and/or Dun and Bradstreet within six months of the release date of the RFR; we requested new reports.

9.1.3. Errors in Open Ratings / Dun and Bradstreet Reports

If a bidder receives the reports but believes they contain errors, it is the bidder's responsibility to contact D&B's Customer Resource Center at 888-299-3118 to report any changes/updates if the issue concerns the "Supplier Qualifier Report" or the "Supplier Analysis Report," and the Open Ratings Coordinator (727-329-1184; orders@openratings.com) at Open Ratings if the problem is with the "Past Performance Evaluation (Supplier Performance Review)" in time to obtain a corrected version to include with the RFR Response.

GDIT did not have errors on the reports.

9.1.4. Explanation Required for Certain Ratings

Bidders whose "Supplier Risk Score" on the Supplier Qualifier Report or Supplier Analysis Report is above 7 must provide a satisfactory explanation to the SST regarding the company's financial position. Bidders whose "Overall Performance Rating" on the Past Performance Evaluation (Supplier Performance Review) is below 80 must provide an explanation to the SST regarding their customer satisfaction score. The SST may disqualify bidders if, in the sole judgment of the SST, the explanations provided are not satisfactory.

Important Note: Failure to have these reports sent to Karen.Robitaille@state.ma.us by Open Ratings and/or Dun and Bradstreet prior to the RFR deadline may result in disqualification of the Proposal. Bidders are advised to contact the Open Ratings Coordinator (727-329-1184; orders@openratings.com) if they have not received their reports by two (2) weeks in advance of the RFR response deadline.

GDIT complies with the RFR specification. An explanation was not required. GDIT received a "3" for Supplier Risk, and an "88" for an Overall performance Rating.

Section 10 – CONTRACTOR PERFORMANCE REQUIREMENTS AND MEASURES

10.1. REMEDIES

The State 911 Department recognizes that it may be impossible to ascertain the amount of damages arising out of failure by the contractor to meet its obligations under the contract. The State 911 Department will assess liquidated damages within ninety (90) days of the breach giving rise to the liquidated damage, provided, however, that the State 911 Department may extend this period for up to ninety (90) additional days by notifying the contractor in writing and stating the reason for the extension. Failure to assess liquidated damages within these timeframes shall not act as a waiver of any other rights or remedies available to the State 911 Department under the contract or at law.

The contractor agrees that such liquidated damages shall be in addition to and without limitation on any rights or remedies which the State 911 Department may have under the contract, or any renewal, or at law or in equity arising out of or related to any other breach by the contractors of its obligations.

Catastrophic System Malfunction

The contractor shall pay to the State 911 Department a credit of $150,000.00 for each catastrophic system malfunction arising out of failure by the contractor to meet its obligations under the contract. Such credits shall be cumulative.

Major System Malfunction

The contractor shall pay to the State 911 Department a credit for each major system malfunction arising out of failure by the contractor to meet its obligations under the contract, as follows: a $25,000 credit if one (1) to five (5) major system malfunctions occur in a month; a $75,000 credit if six (6) to ten (10) major system malfunctions occur in a month; and a $150,000 credit if more than ten (10) major system malfunctions occur in a month. Such credits shall be cumulative.

Notification/Escalation

The contractor shall pay to the State 911 Department a credit for each time the contractor fails to comply with notification/escalation timeframes for catastrophic system malfunctions, major system malfunctions, and high priority system malfunctions, as follows: a credit in the amount of $2,500 if one (1) to five (5) failures occur in a month; a credit in the amount of $5,000 if six (6) to ten (10) failures occur in a month; and a $10,000 credit if more than ten (10) failures occur in a month. Such credits shall be cumulative.

Any and all credits shall appear as a credit on the invoice submitted to the State 911 Department for payment of the services in the month following the month in which the event triggering the credit has occurred, or in the month following the State 911 Department assessment, or in the month following the conclusion of any mediation of a dispute in accordance with Section 14 of the Commonwealth's Terms and Conditions. If such credit is not provided, the State 911 Department may reduce the monthly invoice amount to be paid by the amounts specified. In addition, to the extent that the credits owed to the State 911 Department pursuant to this Section exceed the amounts owed by the State 911 Department to the contractor under the contract, including any and all renewals thereof, the contractor shall promptly make a direct payment to the State 911 Department in such amount.

GDIT will comply with the RFR specification.

Section 11 – INTELLECTUAL PROPERTY RIGHTS

11.1. SOURCE OF PROPERTY

The delivery of services under this RFR will involve intellectual property derived from four different sources: (1) third party software contractors; (2) that developed by the contractor for the open market; (3) that developed by the contractor for other individual clients, or for internal purposes prior to the effective date of the contract entered by the contractor under this RFR and not delivered to any other client of the contractors; and (4) that developed by the

contractor specifically for the purposes of fulfilling its obligations to the State 911 Department under the terms of this RFR. Ownership of the first and second categories of intellectual property will be addressed in separate agreements between the State 911 Department and the owners and resellers of such property. This section of the RFR addresses exclusively ownership rights in the third and fourth categories of intellectual property.

GDIT will comply with the RFR specification.

11.2. CONTRACTOR PROPERTY AND LICENSE

The contractor will retain all right, title and interest in and to all Property developed by it, i) for clients other than the Commonwealth, and ii) for internal purposes and not yet delivered to any client, including all copyright, patent, trade secret, trademark and other intellectual property rights created by contractor in connection with such work (hereinafter the "Contractor Property"). The State 911 Department acknowledges that its possession, installation or use of Contractor Property will not transfer to it any title to such property.

The State 911 Department acknowledges that the Contractor Property contains or constitutes commercially valuable and proprietary trade secrets of the contractor, the development of which involved the expenditure of substantial time and money and the use of skilled development experts. The State 911 Department acknowledges that the Contractor Property is being disclosed to the State 911 Department to be used only as expressly permitted under the terms of the license described in this RFR and any agreement entered with the contractor hereunder. The State 911 Department will take no affirmative steps to disclose such information to third parties, and, if required to do so under the Commonwealth's Public Records Law, Massachusetts General Laws c. 66, § 10, or by legal process, will promptly notify the contractor of the imminent disclosure so that contractor can take steps to defend itself against such disclosure.

Except as expressly authorized in this RFR or any agreement entered hereunder, the State 911 Department will not copy, modify, distribute or transfer by any means, display, sublicense, rent, reverse engineer, decompile or disassemble the Contractor Property.

The contractor grants to the State 911 Department a fully-paid, royalty-free, non-exclusive, non-transferable, worldwide, irrevocable, perpetual, assignable license to make, have made, use, reproduce, distribute, modify, publicly display, publicly perform, digitally perform, transmit and create derivative works based upon the Contractor Property, in any media now known or hereafter known, but only to the extent reasonably necessary for the State 911 Department's exploitation of the deliverables to be developed. The contractor will provide to the State 911 Department the most current copies of any Contractor Property to which the State 911 Department has rights pursuant to the foregoing, including any related documentation.

Notwithstanding anything contained herein to the contrary, and notwithstanding the State 911 Department's use of the Contractor Property under the license created herein, the contractor shall have all the rights and incidents of ownership with respect to the Contractor Property, including the right to use such property for any purpose whatsoever and to grant licenses in the same to third parties.

GDIT will comply with the RFR specification.

11.3. COMMONWEALTH PROPERTY

In conformance with the Commonwealth's Standard Terms and Conditions, on the date on which the State 911 Department reimburses the contractor for a deliverable accepted by the State 911 Department under the terms of this RFR and any agreement entered hereunder, all of the contractor's right, title and interest in all Property developed by contractor under the terms of this RFR and any agreement entered hereunder solely for purposes of creating the deliverables described in such agreements shall pass to and vest in the Commonwealth, including all copyright, patent, trade secret, trademark and other intellectual property rights created by the contractor in connection with such work and any causes of action relating to or based upon such work (hereinafter the "Commonwealth Property"). The Commonwealth Property shall also include all data, including without limitation LIS, ALI, GIS, recordings, stored in the system or obtained from any source whatsoever. The contractor hereby assigns to the Commonwealth, as of the date on which the State 911 Department reimburses the contractor for such deliverables, all intellectual property rights that it may now or hereafter possess in the Commonwealth Property related to such deliverable and all derivative works thereof. The contractor also agrees to execute all documents and take all actions that may be necessary to confirm such rights, including providing any code used exclusively to

develop such deliverables for the State 911 Department and the documentation for such code. The contractor acknowledges that there are currently and that there may be future rights that the Commonwealth may otherwise become entitled to with respect to Commonwealth property that does not yet exist, as well as new uses, media, means and forms of exploitation, current or future technology yet to be developed, and that the contractor specifically intends the foregoing ownership or rights by the Commonwealth to include all such now known or unknown uses, media and forms of exploitation.

The contractor shall take such actions as may be reasonably requested by the State 911 Department to evidence the transfer of ownership of or license to intellectual property rights described in this section, including without limitation, action to transfer licenses from third parties to the Commonwealth. All licenses shall be able to be transferred from one PSAP to another PSAP, and all licenses shall allow for the concurrent use of such licenses by PSAP personnel throughout the Commonwealth.

GDIT will comply with the RFR specification.

11.4. THIRD-PARTY INTELLECTUAL PROPERTY

If the deliverables contain or will contain any third-party intellectual property to which the contractor intends to provide a sublicense, the contractor shall provide copies of all such sublicense agreements as early in the process as possible. The sublicense agreements shall be included in the contractor's initial quotation to the State 911 Department, or, if the requirement to utilize sublicensed intellectual property is not known at the outset of the project, as soon as the requirement becomes known.

Intellectual Property Agreement for Contractor's Employees, Contractors, and Agents

The contractor shall ensure that all contractor personnel providing services under any agreement entered under this RFR that will result in the creation of Commonwealth Property, regardless of whether they are the contractor's employees, contractors, or agents, shall, prior to rendering any services under any agreement entered under this RFR, sign the Intellectual Property Agreement for Contractor's Employees, Contractors and Agents and return signed copies of the same to the State 911 Department prior to the delivery of such services under such agreement.

GDIT will comply with the RFR specification.

11.5. WARRANTY OF NON-INFRINGEMENT

The contractor represents and warrants to the State 911 Department that all goods, services, equipment, software, supplies, any other products provided hereunder do not, and shall not, infringe upon or violate any patent, copyright, trade secret, or proprietary right of any third party. In the event of any claim by a third party against the State 911 Department and/or the Commonwealth, the contractor shall defend, indemnify, and hold harmless the State 911 Department and the Commonwealth against any loss, cost, expense, or liability arising out of such claim, including reasonable attorney fees.

GDIT will comply with the RFR specification.

Section 12 – DOCUMENTS AND REPORTING REQUIREMENTS

12.1. CLEARANCES

The contractor represents and warrants to the State 911 Department that it has obtained all rights, grants, assignments, conveyances, licenses, permissions and authorizations necessary or incidental to any materials owned by third parties supplied or specified by it for incorporation in the deliverables to be developed.

GDIT will comply with the RFR specification.

12.2. SECURITY CLEARANCE

All persons performing services hereunder shall, at the discretion of the State 911 Department, be subject to a criminal background check, including state and national fingerprint checks conducted by the Department of Criminal Justice Information Services.

GDIT will comply with the RFR specification.

12.3. BID BOND

Bidders shall furnish, at their own expense, a bid bond in the amount of five (5) per cent of the total amount of the non-recurring charges identified in Attachment E- Cost Tables, naming the Commonwealth executed by a surety licensed in the Commonwealth. Failure to submit a bid bond shall result in disqualification of the bidder. Bidders shall submit the bid bond in a sealed envelope clearly marked Bid Bond, and shall execute Attachment Q-Certification of Compliance with Bid Bond Requirement certifying that the bid bond names the Commonwealth, is in the amount required, and is executed by a surety licensed in the Commonwealth.

GDIT will comply with the RFR specification.

12.4. PERFORMANCE AND PAYMENT BONDS

The contractor shall furnish, at its own expense, payment and performance bonds naming the Commonwealth executed by a surety licensed in the Commonwealth.

The performance bond shall be in the amount of fifty (50) per cent of the total value of the contract. The payment bond shall be in the full amount of the value of commitments to subcontractors.

The State 911 Department reserves the right to collect on the performance bond if the contractor fails to meet the deadline of June 30, 2016 for complete system installation.

GDIT will comply with the RFR specification.

12.5. INSURANCE

The contractor shall maintain during the term of the contract, and any renewal thereof, insurance in at least the following minimum amounts:

Commercial general liability in the amount of $5,000,000 per occurrence;

Workers' Compensation and employer's liability as required by law; and

Property in the amount of $5,000,000 per occurrence.

The contractor shall furnish the State 911 Department with certificates of insurance evidencing the coverage required herein.

GDIT will comply with the RFR specification.

Section 13 – PRICING/COST TABLE INFORMATION

The pricing for each and every service and commodity required to be furnished under the contract shall be set forth on Attachment E- Cost Tables. The pricing for optional commodities/services shall be set forth Attachment E- Cost Tables: Optional Components.

All rates shall become fixed for the term of the contract, unless there is a material change to a regulation, guideline, standard, or order of the State 911 Department that significantly alters the contractor's ability to provide services, as determined solely in the discretion of the Department. Any renegotiation of rates or pricing resulting from any such material change shall be supported by appropriate and detailed documentation to the satisfaction of the State 911 Department. Further, any renegotiation of rates or pricing at the time of renewal of the contract shall be supported by detailed documentation to the satisfaction of the State 911 Department.

For any and all equipment or services that are not set forth in this RFR, but that may be requested by the State 911 Department during the term of the contract, or any renewal thereof, the contractors shall provide a detailed,

itemized cost estimate for such equipment and/or services that separately displays each component cost, installation cost, maintenance and monitoring cost, and any other cost.

Bidders shall include a cost for each cost element identified on Attachment E- Cost Tables. Bidders shall NOT attempt to incorporate costs in other cost elements and indicate that such costs are included in another cost element. The Cost Table in its entirety shall be completed. If there is no cost for a noted cost element, the bidder shall clearly indicate "no cost" for that element.

Bidders are advised that the monthly charges shall reflect an adjustment using the applicable unit cost noted to reflect the number of PSAPs supported under this contract to determine the overall monthly cost.

Further, bidders may NOT modify the cost table in any way, except that the cell height may be expanded to allow for sufficient space for the entry of the response. Any response that modifies the costs table (other than indicated above) may be considered non-responsive and be given no further evaluation.

Bidders may, however, attach an additional cost table that clearly details the cost associated with any required specification(s) or component(s) that are not addressed in this RFR but are required for the bidder's proposed comprehensive solution for a Next Generation 911 system.

Bidders are advised that any and all cost associated with the provision of goods and services detailed in this RFR not herein identified shall become the sole responsibility of the qualified bidder in fulfillment of its obligations under the awarded contract.

The contractor shall not include the amounts of credits or the risk associated with incurring the amounts set forth in Section 10- Remedies, in the calculation of any price or any cost of the contract or any renewal thereof.

Bidders shall provide a prompt payment discount.

Pricing is provided in a separate volume as required by the RFR.

Section 14 – INVOICING AND PAYMENT

The contractor shall submit a detailed invoice within thirty (30) days of completion of requested goods and/or services and acceptance of deliverable(s), where applicable. Invoices shall, where applicable, clearly detail contract number, project information, number of hours worked, hourly rate, unit cost, service rate(s), itemization of any other costs with supporting documentation, including but not limited to, invoicing from communication service providers to contractor for circuit costs, applicable prompt payment discount, any and all credits applied during that billing cycle and invoice total.

The State 911 Department reserves the right to request modifications to the invoice to ensure that the invoice is clear and concise as to the commodities and services for which it is being billed.

All invoices to and payments from the State 911 Department will be reviewed and processed in compliance with the Commonwealth's standard terms and conditions and bill paying policy as issued by the Office of the State Comptroller and/or any and all applicable local procurement and contracting laws, regulations, rules and policies.

For all services provided to eligible entities, other than the State 911 Department, payment will be the responsibility of the eligible entity. The contractor shall, therefore, agree to coordinate invoicing and payment terms to comply with the requirements of such eligible entities. Invoices shall, at a minimum, clearly detail the product(s), and/or services, number of hours worked, hourly rate (if applicable), itemization of any other costs with supporting documentation, applicable prompt payment discount terms and invoice total.

Bidders are advised that all payments issued by the State 911 Department will be made directly to the contractor, and no payments will be made to any parties other than the contractor for goods and services furnished under this contract.

GDIT will comply with the RFR specification.

Section 15 – RESPONSE EVALUATION CRITERIA

All responses shall be received on or before the submission deadline as defined in this RFR. Late responses will be automatically rejected and will be given no consideration.

Responses will be evaluated in accordance with the following criteria:

- *Bidder's ability to meet the required specifications;*
- *Bidder Interview/Product Demonstration;*
- *Business History;*
- *Demonstration of knowledge, experience and expertise;*
- *Help Desk/NOC operations;*
- *Open Ratings/D&B Report;*
- *Pricing;*
- *Proposed work project plan and project management plan;*
- *Qualifications of Contractor and Key Personnel;*
- *Qualifications of Subcontractors, if any;*
- *Quality and completeness of bidder's overall response;*
- *Supplier Diversity Program Plan; and*
- *Technical merit of the system design and configuration.*
- *The criteria are not listed in order of importance.*

The contractor will be selected based upon the fulfillment of the RFR's qualifications, completion of all the required RFR specifications and attachments listed in this RFR and a determination that the contractor will provide "best value" to the Commonwealth.

The State 911 Department reserves the right to interview any and all bidder(s) to further evaluate the proposed solution, system, capabilities, knowledge, experience and expertise. Further, the State 911 Department reserves the right to require any and all bidder(s) to provide proof of competency in the delivery of the system, applications and appliances being proposed, either by means of site visits to current installations or by means of providing a fully functional demonstration, or otherwise. Bidder(s) will be contacted to schedule a mutually agreed upon date and time should the State 911 Department elect to exercise these options. All interviews will be held at the State 911 Department's offices, and all demonstrations will be held at the State 911 Department's offices, unless otherwise approved by the State 911 Department.

GDIT complies with the RFR specification.

GDIT's proposal meets the submission deadline as defined in the RFR. We understand our response will be evaluated on the quality and completeness of our overall response as well as the evaluation criteria listed above. We have responded completely to all requirements in the RFR and addressed each evaluation criteria throughout our proposal.

We are confident that as a Systems Integrator, our solution offers the Best Value to the State. After conducting an independent, thoughtful evaluation of available systems and services, our selection reflects those that best meet the desired objectives of the Commonwealth. The GDIT team is looking forward to sharing our knowledge, experience and expertise with the state and is prepared for any interviews, site visits, or demonstrations should the state decide to exercise these options.

Section 16 – INSTRUCTIONS FOR SUBMISSION OF RESPONSES

16.1. SUBMISSION OF QUESTIONS

Only questions that are written and submitted via e-mail to Karen.Robitaille@state.ma.us will be accepted and such questions shall include "RFR STATE 911 14-002 Question" in the subject line. No questions will be accepted after 5:00 PM EDT by 5:00 p.m. on Friday, February 28, 2014.

GDIT complies with the RFR specification.

16.2. SUBCONTRACTORS

In addition to the requirements set forth in Attachment A – RFR- Required Specifications, Subcontracting Policies, the response shall disclose whether the bidder intends to use subcontractors to complete some or all of the services under the contract. Bidders shall provide the State 911 Department with a detailed list disclosing every subcontractor, CPE vendor, appliance vendor, software and/or application vendor, partner, or co-bidder whose services, hardware, software, application, or any other item included in their response to this RFR. The response shall identify any such subcontractor(s) on Attachment R2- List of Commodities/Services – Sub-Contractors/Other Vendors, and for each such subcontractor(s) the goods, services, and/or commodities that the bidder intends for the subcontractor to furnish, and shall include executed subcontracts or letters of intent from subcontractors with whom the contractor has subcontracted or intends to subcontract to fulfill the requirements of this RFR. The State 911 Department reserves the right to approve in advance any subcontracted service. The State 911 Department reserves the right to require the contractor to furnish additional supporting documentation to verify that any subcontractor is in good standing, and the State 911 Department reserves the right to require the contractor to replace any and all subcontractors whom the State 911 Department deems, in its sole discretion, are not in good standing. All subcontracts shall be in writing, and copies of such subcontracts shall be provided to the State 911 Department and/or the Commonwealth promptly upon request. Unless otherwise provided by law, neither the State 911 Department nor the Commonwealth is bound by any provisions contained in any subcontract. The contractor shall be responsible for the satisfactory performance and adequate oversight of subcontractors.

No bidder may respond to this RFR with a response or proposal that is based upon or is subject to, in whole or in part, an exclusive relationship or agreement with any subcontractor, CPE vendor, appliance vendor, software and/or application vendor, partner, or co-bidder.

The State 911 Department reserves the right to disqualify any bidder from consideration in the event that said bidder submits a response that is based upon or subject to, in whole or in part, an exclusive relationship or agreement.

GDIT will comply with the RFR specification. Please reference Attachment R2 for our list of identified subcontractors and vendors as of the date of our proposal submittal. Letters of Intent can be found in Appendix K of this proposal.

16.3. SUPPLIER DIVERSITY PROGRAM PLAN

Bidders shall make a commitment to partner with certified Minority- and Women-Owned Businesses and/or a Service-Disabled Veteran-Owned Business Enterprise (SDVOBE) in order to be awarded a Contract. An SDO-certified (formerly SOMWBA-certified) and or SDVOBE Bidder may not list itself or an affiliate as being a Supplier Diversity Partner to its own company. In addition, a narrative statement can be included to supplement the SDP Plan Form providing further details of the SDP commitments. The submission of this narrative statement does not replace the requirement of the SDP Plan Commitment SDP Plan Form #1. ***Bids submitted without an SDP plan Form 1 are subject to rejection without further review.***

The timelines for submission of SDP plan declaration of SDP partners and spending reports are set forth in attachment A: Required Specifications.

Resources available to assist Prime Bidders in finding potential Minority Business Enterprises (MBE) and Women Business Enterprises (WBE) partners can be found on the Supplier Diversity Program Website (www.mass.gov/sdp).

- *Resources available to assist Prime Bidders in finding potential Service-Disabled Veteran-Owned Business Enterprise (SDVOBE) partners can be found on the SDO webpage on the Supplier Diversity Office Website (www.mass.gov/sdo).*
- *The Supplier Diversity Program offers training on the SDP Plan requirements. The dates of upcoming trainings can be found on the OSD Training and Outreach Website. In addition, the SDP Webinar can be located on the Supplier Diversity Program Website (www.mass.gov/sdp).*

GDIT will comply with the RFR specification.

Form 1 is located in Appendix E of this proposal. GDIT is proud of our continuing record in working with small businesses to support government program requirements. GDIT received Highly Successful and Acceptable Ratings in its last three Defense Contract Management Agency (DCMA) Small Business Program audits. In addition, GDIT's Small Business Liaison Officer (SBLO) and our Small Business Program (SBP) Director were both recognized for their Small Business Best Practices. Specifically, DCMA stated that GDIT "has performed in an outstanding manner" and noted our significant outreach efforts to small businesses.

The National Veteran Small Business Coalition awarded GDIT the Champions of Veterans Enterprise Award in 2013 and 2012. This award recognizes significant contributions by an organization dedicated to expanding business opportunities for veterans and service-connected, disabled veterans. The award specifically recognized that we achieved nine percent Veteran Owned and six percent participation for Service-Disabled Veterans. Our corporation has also been presented with the prestigious Nunn-Perry Award (named in honor of former Senator Sam Nunn and Secretary of Defense William Perry) to recognize outstanding mentor-protégé teams formed under the DoD Mentor-Protégé program. In addition, GDIT participates in many other mentor-protégé programs such as Department of Homeland Security (DHS), Small Business Administration (SBA), and others.

16.3.1. Statutory Requirements (FAR 19.702)

Small Business Participation

GDIT will provide the maximum practicable opportunity for small business (SB), certified Minority-and Women-Owned Businesses and/or Service-Disabled Veteran-Owned Business Enterprise (SDVOBE) to meet efficient performance of this contract.

GDIT accomplishes this by encouraging GDIT personnel to work with our corporate SBP director for small business partnerships to actively identify SB, SDB, WOSB, VOSB, SDVOSB, and concerns that can bring value to a GDIT team in support of direct or indirect tasking. This affords small business concerns the opportunity to team with GDIT, or to become a supplier to us. Accordingly, GDIT's success in providing subcontracting opportunities to small business concerns not only results in compliance with our stated goals, but capitalizes on the combined talents and opportunities of GDIT and WOSB, VOSB, and SDVOSB concerns. The GDIT Corporate Small Business Liaison Officer (SBLO) monitors our contracts to ensure compliance with specified goals, informs managers on small business programs, advises them on small business subcontracting regulations, and ensures that GDIT meets its stated subcontracting commitments.

Subcontractor Representation

GDIT will confirm that a subcontractor representing itself has been certified as potential Minority Business Enterprises (MBEs) and Women Business Enterprises (WSBE) by Commonwealth of Massachusetts utilizing their Supplier Diversity Program Website (www.mass.gov/sdp) and www.mass.gov/sdo for Service Disabled Veteran-Owned Business Enterprise (SDVOBE).

Methods Used to Develop Goals and Locate Potential Suppliers

To develop the proposed goals set forth in this Subcontracting Plan, the Project Manager reviews the scope of the technical effort associated with this program to establish potential areas of work to be subcontracted. The GDIT Small Business Liaison Officer, our Director for Small Business Partnerships, as well as the proposed Program Manager in conjunction with our Purchasing department then review the established subcontracting opportunities, or firms known to us that are technically competent in those areas to determine MBE, WBE, and/or SDVOBE. Solicitations are issued and responses are evaluated to determine compliance with the specifications and selection criteria that were identified in the Solicitation. GDIT then uses the proposals of the selected vendors as the basis for MBE, WBE, or SDVOBE goals.

GDIT has access to various source lists, such as the SBA Dynamic Small Business Search, to increase subcontracting opportunities. In addition, GDIT maintains its own electronic searchable Small Business Database that is updated on a regular basis. Information is maintained both in summary and in detail and is referred to before solicitations are distributed to ensure maximum opportunities for targeted groups. The Procurement Technical Assistance Center (PTAC) and other government agencies small business administrators are also sources of information for identifying and locating qualified small business concerns. The GDIT Director for SBP circulates vendor capability statements to the business development and project management personnel of GDIT, in addition to introducing small businesses to our personnel who have requirements to meet.

GDIT has developed a Small Business Resource Site on its intranet containing a wealth of information to support small business searches, teaming, and knowledge. This site includes links to GDIT databases, the DoD's Central Contractor Registration (CCR) Dynamic Small Business Search, and other federal, state, and local small business databases. In addition, the site has links to a variety of resources such as PTAC and Government Small Business Offices. Finally, there is information on small business programs that managers require to understand their small business requirements.

Small businesses are encouraged to meet with GDIT line and marketing managers on an opportunity-driven basis, where there is the potential to team for an upcoming solicitation. The GDIT Director for SBP works with all GDIT divisions and participates in the company's business development initiatives. As a result, the Director facilitates the development of working relationships between small businesses and our program managers by introducing them to the managers, helping them understand the opportunities, and supporting their role within a proposal effort. In addition, the Director provides small businesses with partnering guidelines and information on working with GDIT.

Small businesses interested in working with GDIT can register directly on the GDIT website (http://www.gdit.com). The data submitted can be searched by company name, capability

keywords, North American Industry Classification System (NAICS) codes, business status, technical certifications, location, customer areas, and other parameters. The information submitted to this database is used for consideration of GDIT subcontract needs and partnering opportunities.

16.4. FORMAT OF RESPONSE

REMINDER:

Bidders shall follow the same sectional format of this RFR and provide an individual response to each RFR specification in its response. All responses shall be presented using the same numbering sequence and order used in this RFR.

Bidders shall acknowledge that the bidder accepts the terms and conditions of the RFR specification by clearly stating in the affirmative that the bidder shall "comply" with or "agree" to" the specification. Bidders are advised that a response of "understands" or "understood" may be considered non-responsive. In addition, bidders shall explain in detail how the system shall meet the requirements of the RFR, and a failure to do so may be viewed as an incomplete response.

Bidders shall include in the response a detailed list of all components required for a comprehensive solution. Bidders shall complete Attachment R1 – List of Commodities/Services indicating the components for which the bidder is submitting a response. In addition, bidders shall identify by listing on Attachment R2- List of Commodities/Services – Sub-Contractors/Other Vendors which components, if any, the bidder proposes to be provided by a subcontractor and/or another vendor. The State 911 Department proposes a comprehensive solution for the Next Generation 911 system, and, therefore, bidders shall identify any required specifications or components that are not addressed in this RFR.

Bidders shall NOT include any information relative to costs, cost elements, or pricing in the technical response. All cost and pricing shall be addressed solely in the pricing response.

GDIT complies with the RFR specification.

Completed Attachment R1 and R2 forms are provided in Attachment R1 and R2 of our proposal.

16.4.1. Comm-PASS Transition

The Commonwealth of Massachusetts is transitioning from the Commonwealth's Procurement Access and Solicitation System (Comm-PASS) to COMMBUYS. Effective 5:00 PM on Friday, February 28, 2014, activity on Comm-PASS will be restricted to viewing and downloading of solicitations (and contracts) posted prior to the above- referenced date and time. All Comm-PASS solicitations will migrate and be available in COMMBUYS commencing on Monday, March 24, 2014.

This transition from Comm-PASS to COMMBUYS does not impact the procurement calendar as published in this RFR.

Bidders are advised that any and all documents, including but not limited to, questions and answers, amendments/updates/modifications to this RFR as issued on Friday, February 28, 2014, and/ or notice(s) to bidders, published after 5:00 PM on Friday, February 28, 2014 will be published on the State 911 Department's (Department) website (www.mass.gov/e911).

Bidders will NOT receive an automated notification of any such amendments/changes/notices. It is the sole responsibility of the bidder to monitor the Department's website to obtain all new documents, notifications, changes, notice(s), and/or amendments/modifications/updates associated with the above-referenced solicitation posted after 5:00 PM on Friday, February 28, 2014.

Bidders are advised that submission of a response to this RFR shall address all specifications as detailed in the final version (latest posting) of the RFR. As noted in this RFR, "Bidders shall acknowledge that the bidder accepts the terms and conditions of the RFR specification by clearly stating in the affirmative that the bidder shall "comply" with or "agree" to" the specification."

Finally, bidders are advised that references and requirements regarding Comm-PASS noted in this RFR may be impacted by the introduction of COMMBUYS, and, therefore, bidders may also be required to comply with policies, procedures, and requirements necessitated by the introduction of COMMBUYS.

GDIT complies with the RFR specification.

16.5. REQUIRED FORMS

In order for a response to be considered complete, the following required information and forms shall be completed and submitted:

- *Response addressing all of the specifications as detailed in this RFR*
- *Completed Cost Tables*
- *Standard Contract Form and Instructions**
- *Contractor Authorized Signatory Listing Form**
- *Commonwealth Terms and Conditions**
- *W-9 Request for Taxpayer Identification Number and Certification**
- *Supplier Diversity Program Plan Commitment – SDP Form 1**
- *Prompt Payment Discount Form**
- *Electronic Funds Transfer Form**
- *Intellectual Property Agreement for Contractor's Employees, Consultants and Agents**
- *Attachment Q- Certification of Compliance with Bid Bond Requirement*
- *Open Ratings/Dun & Bradstreet Report*

** Forms can be found on the Forms and Terms tab of the RFR as posted on www.Comm-Pass.com.*

Bidders shall follow the same sectional format of this RFR and provide an individual response to each RFR specification in its response. All responses shall be presented using the same numbering sequence and order used in this RFR.

GDIT complies with the RFR specification.

The required forms are provided in this proposal as follows:

- Appendix A – Standard Contract Form and Instructions
- Appendix B – Contractor Authorized Signatory Listing Form
- Appendix C – Commonwealth Terms and Conditions
- Appendix D – W-9 Request for Taxpayer Identification Number and Certification
- Appendix E – Supplier Diversity Program Plan Commitment – SDP Form 1
- Appendix F – Prompt Payment Discount Form
- Appendix G – Electronic Funds Transfer Form
- Appendix H – Intellectual Property Agreement for Contractor's Employees, Consultants and Agents
- Appendix I – Attachment Q – Certification of Compliance with Bid Bond Requirement
- Appendix J – Open Ratings/Dun & Bradstreet Report

16.6. SUBMISSION OF RESPONSES

Bidders shall submit one (1) clearly marked Original Technical Response, nineteen (19) complete paper copies of the Original Technical Response, and one electronic copy of the Original Technical Response in PDF format by May 23, 2014, 5:00 p.m., Eastern Daylight Time (EDT). Further, bidders shall submit one (1) clearly marked Original Pricing Response, nineteen (19) complete paper copies of the Original Pricing Response, and one electronic copy of the original Pricing Response in PDF format by May 23, 2014, 5:00 p.m., Eastern Daylight Time (EDT).

*Please note that electronic copies are in addition to, and do not substitute for, the hard copies of the Original Response. All signatures on the Original Response shall be the signature of the Authorized Signatory listed on the Contractor Authorized Signature Verification Form. All dates on forms shall be hand-dated. The Original Response shall be double-sided, printed on recycled paper with a minimum post-consumer content of 30% or paper made with tree-free fibers (i.e. paper made from raw materials other than trees, such as kenaf). All responses shall clearly indicate the level of recycled content contained in the paper being used. The use of the following non-recyclable and/or non-reusable materials is strongly discouraged for any **copies** of the Original Response: plastic report covers, plastic dividers, vinyl sleeves, and spiral binding. Please only use three-ringed binders, glued materials, paper clips or staples to secure documents. Bidders shall submit materials in a format that allows for easy removal and recycling of materials. Bidders are also encouraged to use other products that contain recycled content in their response documents. Such products include but are not limited to folders, CDs, envelopes, boxes, etc. Where appropriate, respondents shall note which of these products are made with recycled materials. Bidders shall not submit any unnecessary samples, corporate brochures, attachments, or documents.*

A sealed hard copy of the complete response package is required. Delivery may be made by U.S. Postal Service, courier, or other personal delivery. The outside label shall reference this RFR File Name and Number, RFR State 911 14-002, Next Generation 0-1-1 Emergency Communications System and be addressed to:

Karen Robitaille

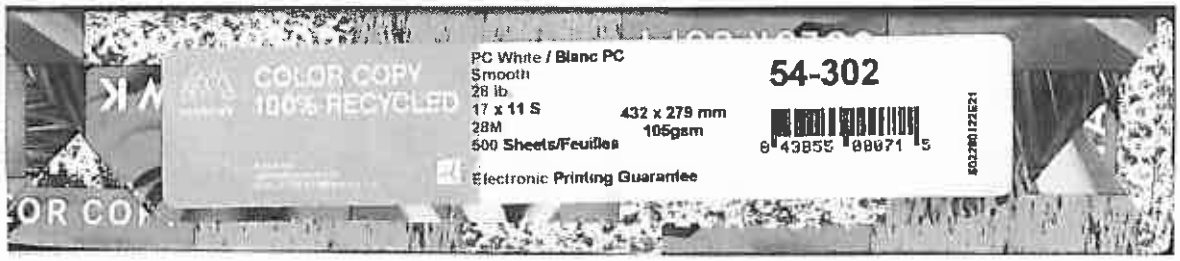
State 911 Department

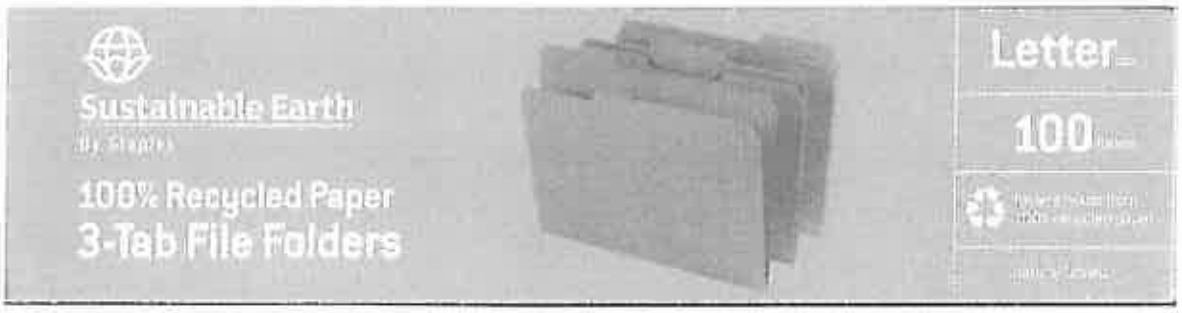
1380 Bay Street, Building C

Taunton, MA 02780

GDIT complies with the RFR specification.

The level of recycled content contained in the paper being used is 100%. The first two images below show the type of paper we used to print this proposal. We also used this paper for the binder and CD inserts. The document holders used in the "Original" printed proposal are made from 100% recycled paper file folders (see third image below). We have also decided not to include tabs in order to reduce the use of non-recycled materials.





Section 17 – DEADLINE FOR RESPONSES AND PROCUREMENT CALENDAR

The critical procurement dates are set forth on the Procurement Calendar below. The State 911 Department reserves the right to modify these dates as needed.

GDIT complies with the RFR specification.

Section 18 – RFR ATTACHMENTS

ATTACHMENT A-	*RFR- REQUIRED SPECIFICATIONS*
ATTACHMENT B-	*RFR-REQUIRED SPECIFICATIONS FOR INFORMATION TECHNOLOGY*
ATTACHMENT C-	*EXECUTIVE ORDER NO. 504*
ATTACHMENT D-	*AT/IT ADAPTIVE LIST*
ATTACHMENT E-	*COST TABLES*
ATTACHMENT F-	*PSAP NETWORK BANDWIDTH*
ATTACHMENT G-	*SECONDARY PSAP DATA*
ATTACHMENT H-	*LIMITED SECONDARY PSAP DATA*
ATTACHMENT I-	*GIS DATA AND DATA SCHEME*
ATTACHMENT J-	*ALI FORMAT*
ATTACHMENT K1-	*PRIMARY PSAP, REGIONAL PSAP, AND RECC DATA*
ATTACHMENT K2-	*PRIMARY PSAP, REGIONAL PSAP, AND RECC DATA*
ATTACHMENT L-	*PROJECT SCHEDULE, DELIVERABLES, AND MILESTONES*
ATTACHMENT M-	*SITE SURVEY PLAN*
ATTACHMENT N-	*TYPES OF SPARE PARTS INVENTORY TO BE MAINTAINED AT LOCATIONS THROUGHOUT THE COMMONWEALTH*
ATTACHMENT O-	*TYPES OF SPARE PARTS INVENTORY TO BE MAINTAINED AT PSAPS*
ATTACHMENT P-	*TYPES OF SPARE PARTS INVENTORY TO BE MAINTAINED AT DATA CENTERS*
ATTACHMENT Q-	*CERTIFICATION OF COMPLIANCE WITH BID BOND REQUIREMENT*
ATTACHMENT R1-	*LIST OF COMMODITIES/SERVICES*
ATTACHMENT R2 -	*LIST OF COMMODITIES/SERVICES – SUB-CONTRACTORS/OTHER VENDORS*
ATTACHMENT S-	*NON-DISCLOSURE AGREEMENT*
ATTACHMENT T-	*COMMONWEALTH NETWORK ASSETS*

GDIT will comply with the RFR specifications.

Responses to RFR attachments, or completed forms where appropriate, follow for each attachment.

Attachment A – RFR – REQUIRED SPECIFICATIONS

GDIT will comply with the RFR specifications.

Attachment B – RFR – REQUIRED SPECIFICATIONS FOR INFORMATION TECHNOLOGY

GDIT will comply with the RFR specifications.

Attachment C – EXECUTIVE ORDER NO. 504

GDIT will comply with the RFR specifications.

Attachment D – AT/IT ADAPTIVE LIST

GDIT will comply with the RFR specifications.

Attachment E – COST TABLES

As required by the RFR, the Cost Tables file is provided separately (electronic copy) and is separately bound (hard copy) in a volume marked "Pricing Response."

Attachment F – PSAP NETWORK BANDWIDTH

Number of 911 Answering Positions	Minimum PSAP Bandwidth Required for Next Generation 911 Payload (KB)	Recommended Bandwidth (KB)
1 (Limited Secondary PSAP)	500	1,500
2	1,000	1,500
3	1,500	3,000
4	2,000	3,000
5	2,500	4,500
6	3,000	4,500
7	3,500	6,000
8	4,000	6,000
9	4,500	7,500
10	5,000	7,500
11	5,500	10,000 (9,000 copper)
12	6,000	10,000 (9,000 copper)
13	6,500	10,000 (10,500 copper)
14	7,000	20,000
15	7,500	20,000

Number of 911 Answering Positions	Minimum PSAP Bandwidth Required for Next Generation 911 Payload (KB)	Recommended Bandwidth (KB)
16 – 20	8,000 ~ 10,000	20,000
21	10,500	20,000
22 – 25	11,000 ~ 12,500	20,000
26 – 30	13,000 ~ 15,000	30,000
31 – 35	15,500 ~ 17,500	30,000
36 – 40	18,000 ~ 20,000	30,000
41 – 44	20,500 ~ 22,000	40,000
45	22,500	40,000
46 – 50	23,000 ~ 25,000	40,000
51+	25,000+	40,000+

Attachment G – SECONDARY PSAP DATA

GDIT will comply with the RFR specifications.

Attachment H – LIMITED SECONDARY PSAP DATA

GDIT will comply with the RFR specifications.

Attachment I – GIS DATA AND DATA SCHEME

GDIT will comply with the RFR specifications.

Attachment J – ALI FORMAT

GDIT will comply with the RFR specifications.

ATTACHMENT K1 – PRIMARY PSAP, REGIONAL PSAP, AND RECC DATA

GDIT will comply with the RFR specifications.

ATTACHMENT K2 – PRIMARY PSAP, REGIONAL PSAP AND RECC DATA

GDIT will comply with the RFR specifications.

Attachment L – PROJECT SCHEDULE, DELIVERABLES, AND MILESTONES

BIDDERS SHALL COMPLETE THE DELIVERABLE DUE DATE WITH A SPECIFIC DATE, (UNLESS THE STATE 911 DEPARTMENT HAS NOTED A DELIVERABLE DUE DATE. THESE DATES SHALL NOT BE ALTERED).

Milestone 1	**System Design and Test Plan Development**		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
1.1	**System Design**		
1.1.1	Develop and Submit to the State 911 Department System Design and Technical Documents	Detailed System Design Documents	Within sixty (60) days of contract award
1.1.2	Develop and Submit to the State 911 Department Detailed Network Design and Technical Documents	Detailed Network Design and Technical Documents	Within sixty (60) days of contract award
1.1.3	Develop and Submit to the State 911 Department Data Center Assessment, System Design and Technical Documents	Data Center Assessment, System Design and Technical Documents	Within thirty (30) days of contract award
1.1.4	Develop and Submit to the State 911 Department Detailed Security Plan	Detailed Security Plan	Within sixty (60) days of contract award
1.1.5	Develop and Submit to the State 911 Department a NOC/Help Desk Operational Manual	NOC/Help Desk Operations Manual	Within sixty (60) days of contract award
1.2	**Test Plan Development**		
1.2.1	Develop and Submit to the State 911 Department System Test Plan, (including Network Test Plan), Test Criteria, Test Cases and Scenarios, and Test Reports for each functional element of the system	System Test Plan (including Network Test Plan), Test Criteria, Test Cases and Scenarios, and Test Reports	9/12/2014
1.2.2	Develop and Submit to the State 911 Department Test Plan, Test Criteria, Test Cases and Scenarios, and Test Reports for GIS Data, Database, and LIS server function, including initial data loading validation, data normalization and load testing	GIS Data, Database, and LIS Server Test Plan, Test Criteria, Test Cases and Scenarios, Test Reports	9/12/2014
1.2.3	Develop and Submit to the State 911 Department Data Center Test	Data Center Test Plan, Test Criteria, Test Cases	9/12/2014

Milestone 1	System Design and Test Plan Development		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
	Plan, Test Criteria, Test Cases and Scenarios, and Test Reports, for each data center	and Scenarios, Test Reports for each data center	
1.2.4	Develop and Submit to the State 911 Department NOC and Monitoring Test Plan, Tests Cases and Scenarios, Test Reports, and document how the system automatically generates trouble tickets and alarming and alerting functions	NOC and Monitoring Test Plan, Test Criteria, Test Cases and Test Scenarios, Test Reports	9/12/2014
1.2.5	Develop and Submit to the State 911 Department Security Test Plan and Test Criteria	Security Test Plan and Security Test Criteria	9/12/2014
1.2.6	Develop and Submit to the State 911 Department Test Schedule	Test Schedule	9/12/2014
		MILESTONE DUE	**October 3, 2014**

Milestone 2	Laboratory Trial and Testing		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
2.1	**Laboratory Trial and Testing Setup**		
2.1.1	Establish Laboratory Staging and Trial Testing Plan	Comprehensive Laboratory Staging and Trial Testing Plan	9/7/2014
2.1.2	Install and Configure Test Equipment, Applications and Appliances and CPE using simulated equipment	Documentation that Test Equipment, Applications and Appliances, and CPE Installed and Prepared for Testing	9/22/2014
2.2	**Laboratory Testing**		
2.2.1	Implement System Test Plan and Correct/Retest as necessary until Test Passed	Final Test Results Report	10/6/2014
2.2.2	Implement GIS, Database, and LIS Server Test Plan and Correct/Retest as necessary until Test Passed	GIS, Database, and LIS Server Test Results Report	10/6/2014
2.2.3	Implement NOC and Monitoring Test Plan and Correct/Retest as	NOC and Monitoring Test Results Report	10/6/2014

Milestone 2	Laboratory Trial and Testing		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
	necessary until Test Passed and NOC processes and procedures refined to reflect results	Updated Documentation	
2.2.4	Implement Security Test Plan	Security Test Results Report	10/6/2014
2.2.5	Event Recording Review and Refinement	Event Recording Results Report demonstrating operational functionality of Event Recording	10/7/2014
2.2.6	Lab Testing Review and adjust any documentation from design phase based on Lab Testing Results	Final Test Acceptance	10/7/2014
2.3	**Change Management Protocol Development**		
2.3.1	Develop and Submit to the State 911 Department Change Management Plan for hardware changes, software updates, software upgrade testing plan, determine change management team, inventory updates and documentation updates.	Change Management Plan	8/24/2014
2.4	**Finalize Network Design and Deployment Plans**		
2.4.1	Revise, Finalize, and Submit to the State 911 Department Network Design based on test results	Final Network Design Document	10/7/2014
2.4.2	Revise, Finalize, and Submit to the State 911 Department Data Center Deployment Plan, and PSAP Deployment Plan based on test results, Deployment Schedule for data centers and PSAPs submitted, planning complete, data centers prepared for commencement of pilot PSAP deployment, ordering schedule finalized	Final Data Center and PSAP Deployment Plan	11/5/2014
2.5	**Training Plan Development**		
2.5.1	Develop Training Plan and Training Materials working with State Department	Training Plan and Training Materials	9/12/2014
2.5.2	Develop Mobile Training Solution working with State 911 Department	Mobile Training Solution Documentation and Demonstration	10/7/2014

Milestone 2	Laboratory Trial and Testing		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
2.5.3	Develop PSAP Pilot Deployment Training Schedule working with State 911 Department	Pilot PSAP Deployment Training Schedule	11/1/2014
2.6	**Pilot Deployment Documentation and Processes**		
2.6.1	Develop and Submit to the State 911 Department Pilot PSAP Deployment Plan, Pilot PSAP Deployment Documentation (including Scheduling, Procurement, Installation, Quality Assurance and Work Order Documentation)	Pilot PSAP Deployment Plan and Pilot PSAP Deployment Documentation	10/27/2014
2.6.2	In conjunction with State 911 Department, Develop and Deliver technical Training Plan and Materials to State 911 Department Systems staff and Develop and Deliver Training to State 911 Department Systems Staff on solution, read-only access to the Help Desk, and Monitoring systems	Training Plan and Materials and Certification of Training for State 911 Department Systems Staff	9/12/2014.
		MILESTONE DUE DATE	**December 3, 2014**

Milestone 3	Data Center Installations and Pilot Deployment Note: Only (2) position PSAPs may be used for the Pilot Deployment		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
3.1	**Data Center Installations**		
3.1.1	Install all equipment, applications and appliances, and software at Data Centers for Pilot Deployment	Equipment, Applications and Appliances, and Software Installed in Data Centers	11/25/2014
3.1.2	Implement Data Center Test Plans (including Stress Test Plan, Data Center Failover Test, including routing failover, physical plant failover, security, application failover, routing, and call distribution	Test Results Reports for all Data Center Test Plans	12/1/2014

Milestone 3	**Data Center Installations and Pilot Deployment Note: Only (2) position PSAPs may be used for the Pilot Deployment**		
Deliverable/ Task Number	**Deliverable/Task Name**	**Deliverable(s)**	**Deliverable Due Date**
3.1.3	Working with EOPSS and State 911 Department, develop Data Center Policies and Procedures for facilities, access procedures, security, notification and escalation processes	Data Center Policy and Procedures	11/24/2014
3.1.4	Review discussions, meetings and modifications as needed resulting from testing and data centers approved by the State 911 Department to be operational	Test Results, Acceptance Report, Site Acceptance Package for each Data Center	On or before Training Center Installation and PSAP Pilot Deployment 12/4/2014
3.2	**Training Center Installation**		
3.2.1	Install all equipment and CPE at Training Centers and connect Training Centers to Data Centers	State 911 Department Training Centers Operational Test Results, Acceptance Report, and Acceptance Package for each Training Center	On or before commencement of PSAP Pilot Deployment 1/28/2015
3.3	**PSAP Pilot Deployment**		
3.3.1	Prepare Six (6) Pilot PSAPs per PSAP Pilot Deployment Plan approved by State 911 Department	Site Cutover Project Plan, Site Survey Form, Staging Test Results for each Pilot PSAP	11/26/2014
3.3.2	Cutover of Six (6) Pilot PSAPs in Pilot Deployment	Cutover Test Results, Post-Cutover Test Results, Cutover Acceptance Report, Site Cutover Acceptance Package for each Pilot Site	2/9/2015
		MILESTONE DUE DATE	**February 17, 2015**

Milestone 4	PSAP Deployment Note: This Milestone includes the Mobile PSAP and from Attachment G - Boston Fire, Springfield Fire and Worcester Fire		
Deliverable/ Task Number	Deliverable/Task Name	Deliverable(s)	Deliverable Due Date
4.1	Cutover of 20 PSAPs	Cutover Acceptance Report for 20 PSAPs	April 30, 2015
4.2	Cutover of 30 PSAPs	Cutover Acceptance Report for 30PSAPs	June 30, 2015
4.3	Cutover of 34 PSAPs	Cutover Acceptance Report for 34 PSAPs	August 31, 2015
4.4	Cutover of 34 PSAPs	Cutover Acceptance Report for 34 PSAPs	October 31, 2015
4.5	Cutover of 28 PSAPs	Cutover Acceptance Report for 28 PSAPs	December 31, 2015
4.6	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	February 28, 2016
4.7	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	April 30, 2016
4.8	Cutover of 35 PSAPs	Cutover Acceptance Report for 35 PSAPs	June 30, 2016
		MILESTONE DUE DATE	June 30, 2016

Attachment M – SITE SURVEY PLAN

GDIT will comply with the RFR specifications.

Attachment N – TYPES OF SPARE PARTS

As stated in Section 8.20.18.1 (Spare Inventory at Contractor Locations), upon award we will identify the spares for each location and submit an updated Attachment N – "Types of Spare Inventory to be Maintained at Locations Throughout the Commonwealth."

A preliminary list of types of spares at Locations Throughout the Commonwealth is located in the table below.

Vendor	Description	Part
Oracle	NNSD 3820 Chassis	NN3820AC
Oracle	NNSD 3820 Power Supply	NN-PS-AC
Oracle	Fan pack assembly	NN3820-O-FPA
HP	Configured DL360p server, 32 Gb, 4x600Mb hd, dual PS	654081-B21
HP	Configured DL320e Server, 8 Gb, 2x500GB HD, dual PS	675597-B21
HP	DL320e 4 Gb, 2x500GB HD	675597-B21
Aculab	Groomer II Chassis	ACS6560RA
Aculab	Groomer II 8 port SIP, ISDN, SS7 module	ACT5800
SpectraCom	Net Clock/GPS Time Server/master clock	9483 - 05,16
EMC SAN	VNXB 1GBASE-T DM MODULE 4 PORT	VDMBM1GCUA
EMC SAN	VNXB 4 PORT 8G FC IO MODULE PAIR	VSPBM8GFFEA
Audio Codes	Mediant 1000B AC power supply	M1KB-PS-AC
Audio Codes	Mediant 1000 Analog Voice Module - Quad FXO	M1K-VM-4FXO
Tripplite	Rack Console with KVM (DCs)	B020-016-17
DSS	3U Recorder Server RAID & Dual hot swap PS	EQSE3U
Cisco	Router	C2901-VSEC/K9
Cisco	Router	C2951-VSEC/K9
Cisco	Switch - 24 port	WS-C3650-24
Cisco	Switch - 48 port	WS-C3650-48
APC	Workstation UPS	SMT1500RM2U
APC	Maintenance Bypass Panel	SBP1500RM
HP	Palladion Probe Server	HP DL160G8
HP	Network Pri nter	HP Laserjet Pro 400
Dell	Workstation	Optiplex 3020
Dell	Soundbar	AX510PA1
Fentek	Programmable Keypad	KPP35U
Logitech	Keyboard	Logitech K120
Logitech	Mouse	Logitech M500
Dell	24" LCD Monitor	P2414H
Tripplite	Rack Console with KVM (LG PSAP)	B020-008-17
Polycom	IP 650 Phone	2200-12651-025
Emergency CallWorks	Audio Interface Unit	EXC100001-NS
Great Lakes	Power Strip	UDS1100

Vendor	Description	Part
Emergency CallWorks	Audio Interface Unit	EXC100001-NS
Lantronix	CAD Interface	UDS1100
Misc. Equipment	Cat 6 Ethernet cable	as required

Attachment O – TYPES OF SPARE PARTS

As stated in Section 8.20.18.2 (Spare Inventory at PSAPs and Data Centers), upon award we will identify the inventory for each site and submit Attachment O – "Types of Spare Inventory To Be Maintained at PSAPs."

A preliminary list of types of spares at PSAPs is located in the table below.

Vendor	Description	Part
Logitech	Keyboard	Logitech K120
Logitech	Mouse	Logitech M500
Great Lakes	Power Strip	UDS1100
Misc. Equipment	Cat 6 Ethernet cable	as required

Attachment P – TYPES OF SPARE PARTS

As stated in Section 8.20.18.2 (Spare Inventory at PSAPs and Data Centers), upon award we will identify the inventory for each site and submit Attachment P – "Types of Spare Inventory To Be Maintained at Data Centers."

A preliminary list of types of spares at Data Centers is located in the table below.

Vendor	Description	Part
Cisco	650W power supply for C-series rack servers	UCSC-PSU-650W
Cisco	650W power supply for C-series rack servers - Standard	PRSM-PSU-650W
Cisco	8GB DDR3-1866-MHz RDIMM/PC3-14900/dual rank/x4/1.5v	UCS-MR-1X082RZ-A
Cisco	1TB SAS 7.2K RPM 2.5 inch HDD/hot plug/drive sled mounted	UCS-HD1T7KS2-E
Cisco	1000BASE-SX SFP transceiver module MMF 850nm DOM	GLC-SX-MMD
Cisco	450W AC Power Supply for Cisco ISR 4451	PWR-4451-AC/2
Cisco	Catalyst 4500X 750W AC back to front cooling 2nd PWR supply	C4KX-PWR-750AC-F/2
Cisco	ASA 5585-X AC Power Supply	ASA5585-PWR-AC
Dell	PowerEdge M620 Blade Server	210-ABVM

Attachment Q – CERTIFICATION OF COMPLIANCE

See Attachment I – Attachment Q- Certification of Compliance with Bid Bond Requirement for GDIT's completed form.

ATTACHMENT R1 – LIST OF COMMODITIES/SERVICES

Bidders shall indicate by a response of "yes" or "no" on the following table those components of a Next Generation 9-1-1 system for which the bidder has proposed to provide in its response to this RFR and the provisioning of a Next Generation 9-1-1 system. Failure to completely and accurately file this attachment may impact the action taken on a bidder's response.

Next Generation 911 System Components	Bidder proposes to provide component Yes or No
8.3 ESI Net	Yes
8.4 Network Security	Yes
8.5 Data Centers	Yes
8.7 Next Generation 911 Architecture	Yes
8.8 Systems Administration	Yes
8.9 Project Management	Yes
8.10 System Reliability & Availability	Yes
8.11 Security, Anti-Virus & Patch Management	Yes
8.12 Training	Yes
8.13 Migration, Deployment, & Installation	Yes
8.15 PSAP and Data Center Moves	Yes
8.16 PSAP and Data Center Inventory	Yes
8.17 Circuit Inventory	Yes
8.18 Inventory Management	Yes
8.19 Electrical, Wiring, and Cable	Yes
8.20 Warranty, Maintenance and Monitoring	Yes
8.22 Removal of CPE, Applications and Appliances	Yes

ATTACHMENT R2 – LIST OF COMMODITIES/SERVICES – SUB-CONTRACTORS/OTHER VENDORS

Bidders shall identify by listing below which components identified on Attachment R1- Commodities/Services, if any, the bidder proposes to be provided by a subcontractor and/or another vendor.

COMMODITY/SERVICE	FUNCTION	PROPOSED SUBCONTRACTOR	COMMENTS
8.3 ESI Net	IP Circuits, Central Offices	Windstream	Commonwealth of MA Service Provider.
8.3 ESI Net	Tertiary Connections	Hughes	
8.3 ESI Net	Network Equipment	Cisco	
8.4 Network Security	Network Servers	SolarWinds	
8.4 Network Security	Network Equipment	Cisco	
8.5 Data Centers	Geo-Diverse Data Center Facilities	Windstream	Commonwealth of MA Service Provider
8.7 Next Generation 911 Architecture	CPE, ACD, Instant Recall, CAD Spill	Emergency CallWorks	NG911 CPE Provider
8.7 Next Generation 911 Architecture	ECRF, LVF, LDB, GIS Data Services	DDTi	NENA Technical Board Member
8.7 Next Generation 911 Architecture	ESRP, Legacy Gateways	Synergem	NENA Technical Board Member
8.7 Next Generation 911 Architecture	Border Control	Oracle/Acme Packet	NENA Technical Board Member
8.7 Next Generation 911 Architecture	Event Logging	DSS	Commonwealth of Mass Voice Recording Provider
8.7 Next Generation 911 Architecture	Time Server	Spectracom	
8.8 Systems Administration	Operational Reporting	Oracle/Acme Packet	NENA Technical Board Member

COMMODITY/SERVICE	FUNCTION	PROPOSED SUBCONTRACTOR	COMMENTS
8.10 System Reliability & Availability	CPE, ACD	Emergency CallWorks	NG911 CPE Provider
8.12 Training	Curriculum Content Development	Windbourne	NENA Technical Board Member
8.13 Migration, Deployment, & Installation	PSAP Circuits	Windstream	Commonwealth of MA Service Provider
8.13 Migration, Deployment, & Installation	Site Preparation, Cutover	Integration Partners	Commonwealth of Ma Business
8.13 Migration, Deployment, & Installation	Site Surveys, Site Preparation, Cutover	Acorn Recording Solutions	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Lab Configuration, Staging	Fotis Networks	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Site Preparation, Cutover	Acadia Communications	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Cabling	Advanced Cabling Concepts	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Installation	Advans IT Services, Inc.	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Installation	DatamanUSA	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Cabling	Metro Telephone	Commonwealth of MA Small Business
8.13 Migration, Deployment, & Installation	Installation	Comtronics	Commonwealth Certified SOWMBA
8.13 Migration, Deployment, & Installation	Installation	Sumaria	Commonwealth of MA Small Business

Bidders shall identify by listing below any required specifications or components that are not addressed in this RFR.

COMMODITY/SERVICE	FUNCTION	PROPOSED SUBCONTRACTOR	COMMENTS
None Identified	N/A	N/A	N/A

Attachment S – NON-DISCLOSURE AGREEMENT

GDIT complied with this requirement on February 12, 2014 with the submission of Non-Disclosure Agreements signed by GDIT employees and its subcontractors with a need to know.

Attachment T – COMMONWEALTH NETWORK ASSETS

GDIT will comply with the RFR specifications.

Appendix A – STANDARD CONTRACT FORM AND INSTRUCTIONS

Appendix B – CONTRACTOR AUTHORIZED SIGNATORY LISTING FORM

Appendix C – COMMONWEALTH TERMS AND CONDITIONS

Appendix D – W-9 REQUEST FOR TAXPAYER IDENTIFICATION NUMBER AND CERTIFICATION

Appendix E – SUPPLIER DIVERSITY PROGRAM PLAN COMMITMENT – SDP FORM 1

Appendix F – PROMPT PAYMENT DISCOUNT FORM

Appendix G – ELECTRONIC FUNDS TRANSFER FORM

Appendix H – INTELLECTUAL PROPERTY AGREEMENT FOR CONTRACTOR'S EMPLOYEES, CONSULTANTS AND AGENTS

Appendix I – ATTACHMENT Q- CERTIFICATION OF COMPLIANCE WITH BID BOND REQUIREMENT

Appendix J – OPEN RATINGS/DUN & BRADSTREET REPORT

GDIT complies with the RFR specification.

GDIT submitted our request for the "Supplier Qualifier Report" and the "Past Performance Evaluation (Supplier Performance Review)" to Open Ratings and Dun and Bradstreet Information Services (D&B) and received a copy of the reports sent to the Commonwealth in a timely manner.

Appendix K – SUBCONTRACTOR LETTERS OF INTENT

Appendix L – INTEGRATED MASTER SCHEDULE (IMS)

Due to its size, GDIT's complete project schedule, or Integrated Master Schedule (IMS), is provided separately (electronic copy) and is separately bound (hard copy) in a volume marked "Appendix L – Integrated Master Schedule (IMS)."

Proposal for:

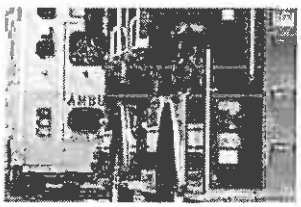
Next Generation 9-1-1 Emergency Communications System

RFR ID: State 911 14-002

Revision 2 / July 28, 2014

Pricing Response



Submitted to:

Karen Robitaille
State 911 Department
1380 Bay Street, Building C
Taunton, MA 02780

E-mail: Karen.Robitaille@state.ma.us

Submitted by:

GENERAL DYNAMICS
Information Technology

77 "A" Street
Needham, MA 02494-2806
www.gdit.com

Table of Contents

Section 1 – COST TABLES

NON-RECURRING COSTS

Milestone 1: System Design and Test Plan Development	
Deliverable/Task Number	**Milestone Payment**
1.1 System Design	
1.1.1	$268,214
1.1.2	$91,527
1.1.3	$117,922
1.1.4	$119,827
1.1.5	$141,864
1.2 Test Plan Development	
1.2.1	$188,609
1.2.2	$163,721
1.2.3	$80,287
1.2.4	$108,444
1.2.5	$77,530
1.2.6	$71,747
TOTAL COST MILESTONE 1: System Design and Test Plan Development	**$1,429,692**

Milestone 2: Laboratory Trial and Testing	
Deliverable/Task Number	**Milestone Payment**
2.1 Laboratory Trial and Testing Setup	
2.1.1	$68,468
2.1.2	$137,904
2.2 Laboratory Testing	
2.2.1	$112,741
2.2.2	$123,972
2.2.3	$47,434
2.2.4	$25,475
2.2.5	$17,684
2.2.6	$151,435
2.3 Change Management Protocol Development	
2.3.1	$95,547
2.4 Finalize Network Design and Pilot Deployment Plan	
2.4.1	$49,338
2.4.2	$43,000
2.5 Training Plan Development	
2.5.1	$45,619
2.5.2	$24,690
2.5.3	$30,239
2.6 Pilot Deployment Documentation and Processes	
2.6.1	$32,063
2.6.2	$20,275
TOTAL COST MILESTONE 2: Laboratory Trial and Testing	**$1,025,884**

Milestone 3: Data Center Installations and Pilot Deployment	
Deliverable/Task Number	**Milestone Payment**
3.1 Data Center Installations	
3.1.1	$9,288,595
3.1.2	$278,953
3.1.3	$53,168
3.1.4	$177,834
3.2 Training Center Installation	
3.2.1	$958,472
3.3 PSAP Pilot Deployment	
3.3.1	Not applicable – Milestone payments will be made upon acceptance of each Pilot PSAP. Payment amounts shall be in the amount set forth in the PSAP Deployment Cost Table below.
3.3.2	Not applicable – Milestone payments will be made upon acceptance of each Pilot PSAP. Payment amounts shall be in the amount set forth in the PSAP Deployment Cost Table below.
TOTAL COST MILESTONE 3: (3.1 and 3.2) Data Center Installation and Pilot Deployment	**$10,757,022**

MILESTONE 4: PSAP Deployment			
PSAP Configuration*	**Quantity**	**Cost Per PSAP**	**Total Cost**
2 Position PSAP	149	$87,824	$13,085,776
3 Position PSAP	55	$101,857	$5,602,135
4 Position PSAP	25	$116,028	$2,900,700
5 Position PSAP	3	$129,973	$389,919
6 Position PSAP	7	$183,966	$1,287,762
7 Position PSAP	3	$307,810	$923,430
8 Position PSAP	2	$321,868	$643,736
9 Position PSAP	2	$355,948	$711,896
13 Position PSAP	1	$431,295	$431,295
14 Position PSAP	1	$456,380	$456,380
21 Position PSAP	1	$557,807	$557,807
45 Position PSAP	1	$973,302	$973,302
Mobile PSAP	1	$434,832	$434,832
TOTAL COST: PSAP DEPLOYMENT			$28,398,970

*Noted pricing shall be for a standard configuration. Components not included in the standard configuration will processed in compliance with costs identify elsewhere on this Attachment E- Cost Tables or agreed upon costs for additional services as defined within the RFR.

OPTIONAL PRICE: Provision of Third Data Center	
Total cost for the provision of a third data center as set forth in Section 8.5 of this RFR	**$4,581,061**

Normalization of GIS DATA	
Total cost for normalization of GIS data required for implementation as set forth in Section 8.6.7 of this RFR	**$1,030,129**

PROJECT MANAGEMENT		
Contract Manager (as set forth in Section 8.9.1)	**Monthly Fee**	**Total Cost (August 4, 2014 –June 30, 2016)**
	$18,811	$432,653
Project Manager (as set forth in Section 8.9.2)	**Monthly Fee**	**Total Cost (August 4, 2014 –June 30, 2016)**
	$24,103	$554,369

TRAINING	
Training Material	**Cost**
Review and Customization of Training Material (as set forth in Section 8.12.1)	$358,724
Training	**Cost per Class**
Operations Training (as set forth in Section 8.12.2)	$3,046
Conversion Training (as set forth in Section 8.12.3)	$3,046
Refresher Training (as set forth in Section 8.12.3)	$3,046
Administrator Training (as set forth in Section 8.12.4)	$1,584

RECURRING COSTS

Customer Support		
Help Desk	**Monthly Fee**	**Total Cost (February 28, 2015– August 3, 2019)**
	$90,648	$4,804,344
NOC	**Monthly Fee**	**Total Cost (February 28, 2015– August 3, 2019)**
	$98,065	$5,197,445
Total Cost Customer Support		**$10,001,789**

Network- Operation and Management and Monitoring			
	Recurring Cost Per Position per Month	**Sub-Total Cost Per Month**	**Total Cost (February 28, 2015– August 3, 2019)**
Operation and Management	$380.11	$312,830	$16,579,990
Monitoring	$202.90	$166,987	$8,850,311
Total Cost Network	**N/A**	$479,817	$25,430,301

NETWORK- MONTHLY CIRCUIT COSTS

THE BIDDER SHALL IDENTIFY ITS PROPOSED SOLUTION FOR THE PROVISION OF PSAP CIRCUITS FOR EACH OF THE CATEGORIES OF PSAP ANSWERING POSITIONS. THE PROPOSED SOLUTION SHALL SUPPORT THE RECOMMENDED BANDWIDTH NOTED BY THE BIDDER. BIDDERS ARE ADVISED THAT THE PROPOSED SOLUTION IDENTIFIED HEREIN SHALL BE UTILIZED FOR IMPLEMENTATION OF THE NEXT GENERATION 911 SYSTEM, UNLESS OTHERWISE DIRECTED BY THE STATE 911 DEPARTMENT. BIDDERS ARE CAUTIONED TO ENSURE THAT THE PROPOSED SOLUTION IS VIABLE AND BEST VALUE.

NETWORK – MONTHLY CIRCUIT COSTS- PRIMARY PATH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Proposed Solution (Circuit Type)**	**Monthly Recurring Cost**
1 (Limited Secondary PSAP)	256 Kb	1.5 Mb	T – 1 Copper	$262
2 – 3	1.0 – 1.5 Mb	1.5 – 3 Mb	T – 1 Copper	$521
4 – 6	2.0 – 3.0 Mb	3 – 4.5 Mb	T – 1 Copper	$868
7 - 10	3.5 – 5.0 Mb	7.5 - 9.0 Mb (Copper) / 20.0 Mb (Fiber)	T – 1 Copper & Ethernet / Fiber	$1,198
11 - 15	5.5 – 7.5 Mb	20.0 Mb	Ethernet / Fiber	$1,473
15 - 20	-	-	-	No Cost
21 – 25	10.5 – 12.5 Mb	20 – 30 Mb	Ethernet / Fiber	$1,534
26 - 30	-	-	-	No Cost
31 - 35	-	-	-	No Cost
36 - 40	-	-	-	No Cost

NETWORK – MONTHLY CIRCUIT COSTS- PRIMARY PATH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Proposed Solution (Circuit Type)**	**Monthly Recurring Cost**
41 - 45	20.5 – 22.5 Mb	40 Mb	Ethernet / Fiber	$2,246
46 - 50	-	-	-	No Cost
51 +	-	-	-	No Cost

NETWORK – MONTHLY CIRCUIT COSTS - SECONDARY PATH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Proposed Solution (Circuit Type)**	**Monthly Recurring Cost**
1 (Limited Secondary PSAP)	256 Kb	1.5 Mb	T – 1 Copper	$1,011
2 – 3	1.0 – 1.5 Mb	1.5 – 3 Mb	Ethernet / Fiber	$1,011
4 – 6	2.0 – 3.0 Mb	3 – 4.5 Mb	Ethernet / Fiber	$1,137
7 - 10	3.5 – 5.0 Mb	7.5 - 9.0 Mb (Copper) / 20.0 Mb (Fiber)	T – 1 Copper & Ethernet / Fiber	$1,350
11 - 15	5.5 – 7.5 Mb	9.0 Mb (Copper) / 20.0 Mb (Fiber)	T – 1 Copper & Ethernet / Fiber	$1,634
15 - 20	-	-	-	No Cost
21 – 25	10.5 – 12.5 Mb	20 – 30 Mb	Fixed Wireless	$2,972
26 - 30	-	-	-	No Cost
31 - 35	-	-	-	No Cost
36 - 40	-	-	-	No Cost
41 - 45	20.5 – 22.5 Mb	40 Mb	Fixed Wireless	$2,972
46 - 50	-	-	-	No Cost
51 +	-	-	-	No Cost

NETWORK – MONTHLY CIRCUIT COSTS - TERTIARY PATH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Proposed Solution (Circuit Type)**	**Monthly Recurring Cost**
1 (Limited Secondary PSAP)	-	-	-	No Cost
2 – 3	-	-	-	No Cost
4 – 6	-	-	-	No Cost
7 - 10	3.5 – 5.0 Mb	7.5 - 9.0 Mb (Copper) / 20.0 Mb (Fiber) / 2.0 Mb Satellite	T-1 Copper, Ethernet / Fiber & Satellite	$5,609
11 - 15	5.5 – 7.5 Mb	9.0 Mb (Copper) / 2.0 Mb (Satellite)	T-1 Copper & Satellite	$8,773
15 - 20	-	-	-	No Cost
21 – 25	10.5 – 12.5 Mb	2.0 Mb	Satellite	$12,536
26 - 30	-	-	-	No Cost
31 - 35	-	-	-	No Cost
36 - 40	-	-	-	No Cost
41 - 45	20.5 – 22.5 Mb	40 Mb	Ethernet / Fiber	$4,881
46 - 50	-	-	-	No Cost
51 +	-	-	-	No Cost

IN ADDITION, BIDDERS SHALL IDENTIFY ANY AND ALL MEANS OF PROVISIONING THE RECOMMENDED BANDWIDTH FOR EACH OF THE CATEGORIES OF PSAP ANSWERING POSITIONS. BIDDERS SHALL ALSO BE REQUIRED TO IDENTIFY THE MONTHLY RECURRING COST ASSOCIATED WITH SAID CIRCUIT TYPE. BIDDERS MAY MODIFY THE TABLE TO IDENTIFY ADDITIONAL MEANS OF PROVISIONING THE RECOMMENDED BANDWIDTH IF THE SPACE PROVIDED IS INSUFFICIENT. NO OTHER CHANGES TO THE COST TABLES SHALL BE MADE.

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
1 (Limited Secondary PSAP)	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
2 – 3	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
4 – 6	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
7 – 10	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
11 - 15	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
15 -20	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
21 - 25	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
26 - 30	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
31 - 35	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
36 - 40	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
41 -45	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
46 - 50	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

NETWORK – SOLUTIONS FOR PROVISIONING RECOMMENDED BANDWIDTH				
Number of 911 Answering Positions	**Minimum PSAP Bandwidth Required for Next Generation 911 Payload**	**Recommended Bandwidth**	**Circuit Type**	**Monthly Recurring Cost**
51 +	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost
	-	-	-	No Cost

Data Centers			
Tier III Facility	**Monthly Fee**	**Quantity**	**Total Cost (December 4, 2014 – August 3, 2019)**
	$20,657	2	$2,313,584
Maintenance of Applications and Appliances	**Monthly Fee**		**Total Cost (December 4, 2015 – August 3, 2019)**
	$67,555	2	$5,944,840
Monitoring of Applications and Appliances	**Monthly Fee**		**Total Cost (December 4, 2014 –August 3, 2019)**
	$395	2	$44,240
Total Cost Data Center		**N/A**	**$8,302,664**

DATA CENTERS (2) NETWORK CONNECTIVITY – PRIMARY PATH			
	RECOMMENDED BANDWIDTH	CIRCUIT TYPE	MONTHLY RECURRING COST
Aggregated ESInet Connections to PSAPs	4 x 1 Gb	Ethernet / Fiber	$9,979
Connections between Data Centers	2 Gb	10 Gb Point-to-Point	$9,007
Connections to the Public Internet	20 Mb	Ethernet / Fiber	$3,110
Connections to the existing Selective Routers	-	-	No Cost
Total Monthly Recurring Cost			$22,096

DATA CENTERS (2) NETWORK CONNECTIVITY – SECONDARY PATH			
	RECOMMENDED BANDWIDTH	CIRCUIT TYPE	MONTHLY RECURRING COST
Aggregated ESInet Connections to PSAPs	1 Gb	Ethernet / Fiber	No Cost
Connections between Data Centers	2 Gb	10 Gb Point-to-Point	$10,757
Connections to the Public Internet	20 Mb	Ethernet / Fiber	$3,110
Connections to the existing Selective Routers	-	-	No Cost
Total Monthly Recurring Cost			$13,867

DATA CENTERS (2) NETWORK CONNECTIVITY – TERTIARY PATH			
	RECOMMENDED BANDWIDTH	CIRCUIT TYPE	MONTHLY RECURRING COST
Aggregated ESInet Connections to PSAPs	-	-	No Cost
Connections between Data Centers	2 Mb	Satellite	$11,469
Connections to the Public Internet	-	-	No Cost
Connections to the existing Selective Routers	-	-	No Cost
Total Monthly Recurring Cost			$11,469

Legacy PSAP Gateway		
Provision of Legacy PSAP Gateway (as set forth in Section 8.7.11.2 of this RFR)	**Monthly Fee**	**Total Cost (February 28, 2015 –August 3, 2019)**
	No Cost	No Cost

Database Services			
Provision of Database Services (as set forth in Section 8.7.13 of this RFR)	**Cost per 1,000 Records per month**	**Total Cost Per Month**	**Total Cost (February 28, 2015 – August 3, 2019)**
	$25	$87,342	$4,629,126
Subscription Services (as set forth in Section 8.7.13 of this RFR)	**Cost per 1,000 Records: Daily Update**	**Cost per 1,000 Records: Weekly Update**	**Cost per 1,000 Records: One-Time Extract**
	No Cost	No Cost	No Cost

Customer Premises Equipment Maintenance and Monitoring				
	Cost Per PSAP Per Month	**Quantity**	**Total Cost Per Month**	**Total Cost (February 28, 2015 – August 3, 2019)**
Maintenance	$197.05	**823**	$162,172	$8,595,116
Monitoring	$24.73	**823**	$20,353	$1,078,709
Total Cost CPE Maintenance And Monitoring		**N/A**		**$9,673,825**

MOBILE PSAP			
	Unit	**Per Unit Cost**	**Total Cost (August 4, 2015 – August 3, 2019)**
MAINTENANCE			
	Monthly	$1,464	$70,272
MONITORING			
Standby Monitoring (not deployed)	Monthly	No Cost	No Cost
Active Monitoring (deployed)	Daily	$16	Not Applicable
Active Monitoring (deployed)	Weekly	$110	Not Applicable
Active Monitoring (deployed)	Monthly	$438	Not Applicable
Active Monitoring (deployed)	Multiple Months	$438	Not Applicable
Total Cost Mobile PSAP	**N/A**		**$70,272**

GRAND TOTAL:	**$58,107,977**
RECURRING COSTS (CUSTOMER SUPPORT, NETWORK, DATA CENTERS, LEGACY PSAP GATEWAY, DATABASE, MAINTENANCE & MONITORING OF CPE, MOBILE PSAP)	

Optional Third Data Center		
Tier III Facility	**Monthly Fee**	**Total Cost (December 4, 2014–August 3, 2019)**
	$14,993	$839,608
Maintenance	**Monthly Fee**	**Total Cost (December 4, 2015 –August 3, 2019)**
	$68,750	$3,025,000
Monitoring	**Monthly Fee**	**Total Cost (December 4, 2014–August 3, 2019)**
	$165	$9,240
Total Cost Optional Data Center		$3,873,848

Optional Third Data Center Network Connectivity – PRIMARY PATH			
	RECOMMENDED BANDWIDTH	CIRCUIT TYPE	MONTHLY RECURRING COST
Aggregated ESInet Connections to PSAPs	2 x 1 Gb	Ethernet / Fiber	$4,990
Connections between Data Centers	2 Gb	10 Gb Point-to-Point	$15,298
Connections to the Public Internet	20 Mb	Ethernet / Fiber	$778
Connections to the existing Selective Routers	-	-	No Cost
Total Monthly Recurring Cost			$21,066

Optional Third Data Center Network Connectivity – SECONDARY PATH			
	RECOMMENDED BANDWIDTH	CIRCUIT TYPE	MONTHLY RECURRING COST
Aggregated ESInet Connections to PSAPs	1 Gb	Ethernet / Fiber	No Cost
Connections between Data Centers	-	-	No Cost
Connections to the Public Internet	20 Mb	Ethernet / Fiber	$778
Connections to the existing Selective Routers	-	-	No Cost
Total Monthly Recurring Cost			$778

Optional Third Data Center Network Connectivity – TERTIARY PATH			
	RECOMMENDED BANDWIDTH	CIRCUIT TYPE	MONTHLY RECURRING COST
Aggregated ESInet Connections to PSAPs	-	-	No Cost
Connections between Data Centers	2 Mb	Satellite	$11,522
Connections to the Public Internet	-	-	No Cost
Connections to the existing Selective Routers	-	-	No Cost
Total Monthly Recurring Cost			$11,522

Project Management		
Contract Manager (as set forth in Section 8.9.1)	**Hourly Fee**	**Total Cost (July 1, 2016 –August 3, 2019)**
	$122.64	$726,051
Project Manager (as set forth in Section 8.9.2)	**Hourly Fee**	**Total Cost (July 1, 2016 –August 3, 2019)**
	$157.40	$931,808

Time and Material Rates		
Personnel Category	**Level of Expertise**	**Hourly Rate**
Network Architect	Senior Level	$309
Network Engineer	Senior Level	$309
Technician I	Intermediate Level	$242
Technician II	Senior Level	$387
Field Technician I	Intermediate Level	$217
Field Technician II	Senior Level	$247
Supervisory Service Technician/Manager	Principal Level	$532
Electrician – Apprentice	Junior Level	$40
Electrician	Intermediate Level	$56

Time and Material Rates		
Personnel Category	**Level of Expertise**	**Hourly Rate**
Master Electrician	Senior Level	$68
Cabling Technician	Intermediate Level	$155

Customer Premises Equipment	
New 2 Position PSAP (standard configuration)	**UNIT COST**
Hardware	$40,694
Hardware Installation	$15,325
Software	$15,027
Software Installation	$15,325
Additional PSAP Position (standard configuration)	**UNIT COST**
Hardware	$6,474
Hardware Installation	$7,662
Software	$7,514
Software Installation	$7,662

Limited Secondary PSAP Customer Premises Equipment	
	UNIT COST
Hardware	$11,866
Hardware Installation	$7,662
Software	$1,267
Software Installation	$7,662

Optional Components		
	Unit Cost	**Monthly Maintenance Cost**
Administrative Position	$1,748	No Cost
Audio Monitoring	$0	No Cost
Black & White Laser Jet Printer (equivalent to HP P2035)	$309	No Cost
Color Laser Jet Printer (equivalent to HP Pro 400)	$386	No Cost
Digital Logging Recorder (i3 Compliant)	$14,792	$184
Headset – wired	$143	No Cost
Headset – wireless	$229	No Cost
Handset – wired	$330	No Cost
Keyboard – wired	$14	No Cost
Keyboard Arbitrator	$105	No Cost
Monitor(equivalent to make/model provided with system)	$322	No Cost
Mouse – wired	$30	No Cost
Network Equipment (Routers, Switches, Firewalls, Intrusion Protection/Intrusion Detection)	$343,858	No Cost
PC cable extension kit for video, keyboard and mouse	$35	No Cost
PC Speakers	$21	No Cost
Remote Ringer	$228	No Cost
Administrative IP Phone Set	$330	No Cost
Uninterruptable Power Supply for a 1 Position PSAP	$3,585	$36

Optional Components		
	Unit Cost	Monthly Maintenance Cost
Uninterruptable Power Supply for a 2 Position PSAP	$4,523	$45
Uninterruptable Power Supply for a 3 Position PSAP	$5,460	$55
Uninterruptable Power Supply for a 4 Position PSAP	$6,397	$64
Uninterruptable Power Supply for a 5 Position PSAP	$7,334	$73
Uninterruptable Power Supply for a 6 Position PSAP	$8,272	$83
Uninterruptable Power Supply for a 7 Position PSAP	$9,209	$92
Uninterruptable Power Supply for a 8 Position PSAP	$10,146	$101
Uninterruptable Power Supply for a 9 Position PSAP	$11,084	$111
Uninterruptable Power Supply for a 10 Position PSAP	$12,021	$120
Uninterruptable Power Supply for a 11 Position PSAP	$12,958	$130
Uninterruptable Power Supply for a 12 Position PSAP	$13,895	$139
Uninterruptable Power Supply for a 13 Position PSAP	$14,833	$148
Uninterruptable Power Supply for a 14 Position PSAP	$15,770	$158

Optional Components		
	Cost	Monthly Maintenance Cost
Uninterruptable Power Supply for a 15 Position PSAP	$16,707	$167

Uninterruptable Power Supply for a 21 Position PSAP	$22,331	$223
Uninterruptable Power Supply for a 45 Position PSAP	$44,825	$448

Section 2 – PROPOSAL ASSUMPTIONS

The scheduled delivery dates for the Milestones 1–4 as set out in the RFR, are subject to the award of a contract upon the dates set out in Section 17 of the RFR.

GDIT assumes we will be provided access and information pertaining to existing Commonwealth Data Centers for the feasibility assessment within 7 day of award.

GDIT assumes that all equipment installed by GDIT will remain in the same configuration and location as it was when deployed and accepted by the Commonwealth, in order to retain system integrity.

GDIT assumes we will mutually agree on the schedule for review and approval of deliverable submissions by the Commonwealth.

Deleted.

The GDIT solution does not require the provisioning of bandwidth; therefore, no monthly cost has been included within the cost tables.

GDIT pricing for Data Center connectivity requires the ordering of both primary path and secondary path.

Based on the RFR requirement to provide secondary ESInet connection at PSAPs with 6 or greater positions, GDIT assumes that (optional) tertiary ESInet connections are requested for PSAPs with 7 or greater call taker positions.

Deleted.

The "Grand Total: Recurring Costs" does not include the monthly circuit costs as this element was not listed to be summed up within the total recurring costs.

The Time and Materials (T&M) rates provided are considered ceiling rates. GDIT will discount off these rates on a case-by-case basis as effort is required.

GDIT assumes that the existing selective routers will be end-of-service in 2016 and that the proposed NG9-1-1 data centers will be designated by the Commonwealth as the Public Safety Designated Termination Points (DTPs).

GDIT assumes that Originating Service Providers (OSPs) are required to connect to the Commonwealth's designated DTP at their own cost and in a timeframe that supports the Commonwealth's deployment schedule.

GDIT's proposed solution and pricing includes termination devices to support TDM (CAMA, SS7, and T1) and IP termination. Where TDM is the agreed termination with any OSP, GDIT assumes that the OSP will allow colocation of GDIT-provided TDM gateways and provide IP transport to both designated data centers at the OSP's cost. Also, where IP is the agreed termination type with any OSP, GDIT assumes that the OSP will terminate their IP circuits at both designated data centers at the OSP's cost. Today, an OSP's DTP is at selective router location and the OSP is responsible for the cost of delivery to that point. With the DTP being

changed to data centers, the same assumptions are applied regarding the OSP responsibility of the cost.

The Commonwealth of Massachusetts
EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
STATE 911 DEPARTMENT
1380 Bay Street, Building C ~ Taunton, MA 02780-1088
Tel: 508-828-2911 ~ TTY: 508-828-4572 ~ Fax: 508-828-2585
www.mass.gov/e911

DEVAL L. PATRICK
Governor

ANDREA CABRAL
Secretary of Public Safety and Security

FRANK POZNIAK
Executive Director

July 23, 2014

Mr. Earl Doggett
General Dynamics Information Technology
77 A Street
Needham, MA 02494

RE: RFR State 911 14-002
Next Generation 911 Products and Services

Dear Mr. Doggett:

In connection with the response received from General Dynamics Information Technology ("GDIT") to the above-referenced request for response ("RFR"), the State 911 Department ("Department") requests clarification on the items identified below.

Network Design

The RFR response (p. 32) refers to MOB carrier Ethernet links. Please explain what the term MOB means.

Optional Third Data Center

The RFR (section 8.5) provides that the optional third data center shall be maintained at one (1) software revision prior to the production system version for purposes of rolling back the system if necessary. Your response to the RFR did not address this requirement. Please address this requirement.

Data Centers: Active-Active Model

Please confirm that the data centers will be deployed in an "active-active model between data centers for each application." (Please refer to page 68 of the RFR response).

Geographic Information Systems

The RFR response (p. 91) provides two alternatives for orthophoto interface. Please note that MassGIS will provide the GIS data and the tiles, and opts for the data to be served from within the ESInet. Please confirm that this configuration is included in the proposal.

Next Generation 911 Architecture: Future-proofing

The RFR response (p. 103) states that, "with few exceptions," increases in capacity are supported through increase in software licenses only. Please identify the exceptions.

Data Center Staffing

Please describe the qualifications of the staff that will be on-site at the data centers during the patching of servers.

Configuration of UPS

The RFR (section 8.19.1) requires the contractor to provide and maintain a thirty (30) minute UPS for all equipment supplied at the PSAP and at the data centers and for all DLRs. A hard bypass unit is required. The RFR response (p. 319) states that there will be a UPS with a hard bypass unit. During the interview, however, GDIT mentioned a standalone UPS by position at each workstation. Please confirm that a hard bypass unit is provided. Further, please confirm that there is a single centralized UPS. For clarity, the current Massachusetts PSAP configuration includes a single centralized hardwired UPS that all positions are hardwired back to. The Department would like to reutilize the existing wiring infrastructure by installing a similar type UPS system.

Alarm Categories

The RFR response (p. 208) is missing text and appears to contain typographical errors. Please revise the response to this section.

PS/ALI

Please explain how GDIT shall communicate the transition to the MLTS operators throughout the Commonwealth as part of the transition plan from the legacy system. Please refer to section 8.7.24 of the RFR.

Training: Use of Mobile Remote Training Systems

Please confirm GDIT's understanding that the State 911 Department's mobile PSAP will not be used for training. However other mobile training solutions will be provided by GDIT.

Maintenance

Please confirm that the five (5) dedicated GDIT Regional Supervisory Technicians referenced in the RFR response (p. 352) shall be the prime hands on resources for all aspects of the project.

Springfield Data Center

Please confirm that the renovations required to bring the proposed Springfield Data center to Tier III compliance shall be completed on or before November 25, 2014 (the date set forth in the RFR response for the Data Center Installation in Milestone 3).

Offsite Storage for Event Loggers

Please confirm that fourteen (14) terabytes of offline storage shall be available to backup event loggers.

Mobile PSAP CPE Monitoring

The RFR (section 8.7.32.9) requires that the contractor provide standby mobile PSAP monitoring when the mobile PSAP is inactive. Please note that the mobile PSAP is shut down (off) when it is not deployed. The Department does not require the mobile PSAP to be monitored when the mobile PSAP is shut down and powered off. The Department notes that the cost set forth in the Cost Proposal for Mobile PSAP Standby Monitoring identifies a significantly higher cost when the mobile PSAP is not deployed (turned off) than the cost for active monitoring when the mobile PSAP is deployed (on). Please revisit your pricing with this understanding.

Limited Secondary PSAP CPE

Please identify the equipment and any associated installation costs that are included in the quoted price for limited secondary PSAP CPE.

Tertiary Path (Data Centers and PSAPs)

Please identify the cost elements that are included in the monthly recurring costs. Please address whether the satellite equipment and installation costs are included.

Reuse of Existing Equipment

Please confirm your agreement that, to the extent that the parties agree that existing equipment (such as cabinets) is able to be reused for the deployment, a price reduction will be negotiated by the parties.

Additional Services

GDIT's response to section 8.21 Additional Services of the RFR presents EMC VMWare and GDIT University Web-based Learning/Training Solutions. GDIT's cost proposal, however, did

not contain pricing for these additional services. Please provide the pricing structure for EMC VMWare and GDIT University Web-based Learning/Training Solutions.

Forms

Please complete the attached proof of authentication of signature for Terrance Ward.

RFR Compliance

Please confirm that wherever the statement "will comply with the RFR specification" appears, GDIT agrees that such response and such statement shall be deemed to state "shall comply with the RFR specification" and shall be considered to mean that GDIT shall comply with the RFR requirement as stated in the RFR or as further clarified in such response.

Please provide a response to all items no later than 12:00 PM on Monday, July 28th. The response may be submitted to my attention via e-mail with the original being mailed to my attention at the address above. **Please also identify no later than close of business on Thursday, July 24th, any significant areas of concern that may impact your ability to respond to each of the above items in the noted timeframe.**

Please feel free to contact me at (508) 821-7221 should you have any questions.

Sincerely,

Karen Robitaille

Karen Robitaille (TFA)
Finance Director

cc: Stephen Woodworth, Contracts Manager, GDIT

GENERAL DYNAMICS
Information Technology

DELIVERED BY HAND AND EMAIL (karen.robitaille@state.ma.us)

July 28, 2014

Ms. Karen Robitaille
State 911 Department
1380 Bay Street, Building C
Taunton, MA 02780

Subject: RFR STATE 911 14-002 – Response to Letter Dated July 23, 2014
Enclosures: Revised Pricing Response, Proof of Authentication of Signature form for Terrance Ward

Dear Ms. Robitaille:

General Dynamics Information Technology, Inc. (GDIT) is pleased to submit its response to the request for clarifications as set out in the State 911 Department's letter dated July 23, 2014. GDIT hereby submits the requested clarifications as follows:

Network Design

The RFR response (p. 32) refers to MOB carrier Ethernet links. Please explain what the term MOB means.

"MOB" is a typographical error and should be replaced with "10 GB" and "20 GB" respectively. The sentence on p. 32 should read: "PSAPs containing 20 positions or more will have minimum redundant **10 GB** carrier Ethernet links to the redundant WAN architecture as well as a **20 GB** fixed wireless tertiary path where line-of-sight is available (see Figure 6)." Additionally, on p. 33, the Figure 6 caption should read: "PSAPs with 20+ operator positions will have a minimum of **10 GB** dual redundant access circuits."

Optional Third Data Center

The RFR (section 8.5) provides that the optional third data center shall be maintained at one (1) software revision prior to the production system version for purposes of rolling back the system if necessary. Your response to the RFR did not address this requirement. Please address this requirement.

GDIT shall comply with the RFR requirement that the optional third data center be maintained at one (1) software revision prior to the production system version for purposes of rolling back the system if necessary. GDIT believes there can be value in this practice in providing protection against software-induced corruptions. GDIT does recommend that potential differences associated with maintenance, patches, database, and configurations be reviewed and understood to ensure that any potential risks are understood and mitigated.

Data Centers: Active-Active Model

Please confirm that the data centers will be deployed in an "active-active model between data centers for each application." (Please refer to page 68 of the RFR response).

GDIT confirms that we shall comply with the requirement to deploy the data centers in an active-active model. GDIT will load-balance traffic across the two primary data centers, ensuring that the alternate data

77 A Street
Needham, MA 02494-2806
Tel: 781-400-7493
Fax 781-455-5100

center is active and ready to receive traffic from the other data center should a network, system, or site failure occur.

Geographic Information Systems

The RFR response (p. 91) provides two alternatives for orthophoto interface. Please note that MassGIS will provide the GIS data and the tiles, and opts for the data to be served from within the ESInet. Please confirm that this configuration is included in the proposal.

GDIT confirms the referenced configuration is included in our proposed solution. GDIT's proposed solution includes the placement of an ArcGIS server in each data center that will receive GIS data and orthophotos from Mass GIS and publish to appropriate systems from within the ESInet.

Next Generation 911 Architecture: Future-proofing

The RFR response (p. 103) states that, "with few exceptions," increases in capacity are supported through increase in software licenses only. Please identify the exceptions.

The exceptions noted are:

- The PIF (gateways) utilize TDM interfaces that require the incremental addition of interface cards and/or chassis based on the number and types of interfaces. The number of TDM interfaces is expected to decline over time, rather than grow.
- Additional call taker positions will require the addition of the call taker workstation configurations.

Data Center Staffing

Please describe the qualifications of the staff that will be on-site at the data centers during the patching of servers.

The staff on-site at the data centers during the patching of servers are systems administrators who have skills and certifications (as appropriate for OEM/technology) in the principles, methods, and techniques for NG9-1-1 systems administration.

Configuration of UPS

The RFR (section 8.19.1) requires the contractor to provide and maintain a thirty (30) minute UPS for all equipment supplied at the PSAP and at the data centers and for all DLRs. A hard bypass unit is required. The RFR response (p. 319) states that there will be a UPS with a hard bypass unit. During the interview, however, GDIT mentioned a standalone UPS by position at each workstation. Please confirm that a hard bypass unit is provided. Further, please confirm that there is a single centralized UPS. For clarity, the current Massachusetts PSAP configuration includes a single centralized hardwired UPS that all positions are hardwired back to. The Department would like to reutilize the existing wiring infrastructure by installing a similar type UPS system.

GDIT confirms that we will deploy a centralized UPS to support both the back-office systems and 9-1-1 call taker equipment installed at the PSAPs. The centralized UPS configuration for each PSAP location will include a hard bypass as required by the RFR. The UPS configuration will include the appropriate quantity

of battery modules necessary to support the site-specific equipment load for a 30-minute run time. The proposed solution will be of a similar type to the existing UPS.

All call taker positions will be hard-wired back to the centralized UPS. GDIT will re-use the existing electrical infrastructure (i.e., wiring, conduit, power panel, and outlets) to the maximum extent feasible. If any portion of the existing infrastructure is deemed inadequate, GDIT will note this in its site survey report and provide recommendations to the Commonwealth for the upgrades necessary to support the new UPS architecture.

Alarm Categories

The RFR response (p. 208) is missing text and appears to contain typographical errors. Please revise the response to this section.

GDIT concurs. The Alarm Categories section should read as follows:

> **8.8.6. Alarm Categories**
> Our proposed system fully complies with the RFR specifications; includes all specified categories of alarms; allows the administrator to configure notification thresholds; and also allows the creation of new alarm categories. Additionally, our solution is capable of sending notifications of alarm conditions to any specified personnel or agencies.
>
> GDIT's network management solution is also further detailed in Section 8.20.7.3 (Network Security and Operations Center) and Section 8.20.9 (Monitoring of Applications, Appliances, and CPE).

PS/ALI

Please explain how GDIT shall communicate the transition to the MLTS operators throughout the Commonwealth as part of the transition plan from the legacy system. Please refer to section 8.7.24 of the RFR.

GDIT will work in collaboration with the State 911 Department to gain access to the list of all current PS/ALI users from the ALI operator. As a backup, GDIT will also identify all MLTS operators within the Commonwealth who have a registered NENA Company ID, as required per 560 CMR 4.00 of the M.G.L.c.6A, 18J.

The consolidated list of PS/ALI users will be used by GDIT to provide notification of the changes in PS/ALI update methodology, and to communicate the new procedures and the availability of training and support resources. The communication method(s) and protocol will be coordinated with the Commonwealth to ensure complete MLTS operator awareness, and are expected to include:

- Direct written correspondence
- Email notification
- Phone
- Redirection of traffic from existing PS/ALI website to new website (as supported by PS/ALI owner)
- Other communications methods as needed

GDIT will also track and report on communication activities with each of the MLTS Operators and their participation in support and training activities.

Training: Use of Mobile Remote Training Systems

Please confirm GDIT's understanding that the State 911 Department's mobile PSAP will not be used for training. However other mobile training solutions will be provided by GDIT.

GDIT fully understands that the State 911 Department's mobile PSAP will not be used for training. GDIT's solution provides for a mobile remote training system.

Maintenance

Please confirm that the five (5) dedicated GDIT Regional Supervisory Technicians referenced in the RFR response (p. 352) shall be the prime hands on resources for all aspects of the project.

The five (5) dedicated GDIT Regional Supervisory Technicians will be the hands-on primary leads supported by other fully trained and qualified personnel as needed to complete project tasks.

Springfield Data Center

Please confirm that the renovations required to bring the proposed Springfield Data center to Tier III compliance shall be completed on or before November 25, 2014 (the date set forth in the RFR response for the Data Center Installation in Milestone 3).

Following review of the Commonwealth-existing data centers and recommendations made, should the Springfield Data Center be the selected location, GDIT will work with the facility owner to ensure the Tier III upgrades are complete by November 25, 2014.

Offsite Storage for Event Loggers

Please confirm that fourteen (14) terabytes of offline storage shall be available to backup event loggers.

GDIT confirms that 14 TB of external storage is provided as backup and retention storage for all systems within the ESInet, including the event logger.

Mobile PSAP CPE Monitoring

The RFR (section 8.7.32.9) requires that the contractor provide standby mobile PSAP monitoring when the mobile PSAP is inactive. Please note that the mobile PSAP is shut down (off) when it is not deployed. The Department does not require the mobile PSAP to be monitored when the mobile PSAP is shut down and powered off. The Department notes that the cost set forth in the Cost Proposal for Mobile PSAP Standby Monitoring identifies a significantly higher cost when the mobile PSAP is not deployed (turned off) than the cost for active monitoring when the mobile PSAP is deployed (on). Please revisit your pricing with this understanding.

GDIT incorrectly allocated a portion of its network monitoring cost within the "Mobile PSAP" section in the "Standby Monitoring" row (Pricing Response, p. 21). These costs are part of GDIT's total proposed monitoring solution and have been reallocated to the "Network-Operation and Management and

Monitoring" section of recurring costs in the "Monitoring" row (Pricing Response, p. 6). The words "No Cost" are now in the "Standby Monitoring" row of the "Mobile PSAP" section as there is no additional cost required above what GDIT has already proposed.

Limited Secondary PSAP CPE

Please identify the equipment and any associated installation costs that are included in the quoted price for limited secondary PSAP CPE.

The table below identifies the elements that are included within the hardware and software equipment pricing provided by GDIT. The hardware and software installation prices provided within the "Limited Secondary PSAP Customer Premises Equipment" table (Pricing Response, p. 26) include the performance of site survey, site preparation, installation, configuration, testing and cutover.

Item Description	Vendor	Quantity
Router	Cisco	1
Switch	Cisco	1
Network Printer	HP	1
Sound Point IP 650	Polycom	1
SIPStation License (Per Position)	Emergency CallWorks	1
Cable Assembly, Cat5E, Various Lengths	Misc	1

Tertiary Path (Data Centers and PSAPs)

Please identify the cost elements that are included in the monthly recurring costs. Please address whether the satellite equipment and installation costs are included.

GDIT has proposed three types of tertiary network connections to support network redundancy:

- **Fixed Wireless.** Available only to select Boston area PSAPs. The only cost components for Fixed Wireless are monthly recurring costs that are included in GDIT's proposed price.
- **Alternate Carrier Terrestrial Connections.** Available at select PSAPs. The only cost components for Alternate Carrier Terrestrial Connections are monthly recurring costs that are included in GDIT's proposed price.
- **Satellite Connectivity.** GDIT has proposed satellite services at all PSAPs where other tertiary connections are not available. Satellite provides point-to-point connections between selected PSAPs and the data center, with each route having four cost components:
  - Hardware and installation of base station at the data center
  - Monthly recurring costs for the data center uplink bandwidth
  - Hardware and installation of base station at the PSAP
  - Monthly recurring costs for the PSAP bandwidth

  The maximum available bandwidth on the PSAP uplink is 2 MB, and the maximum available bandwidth on the data center uplink is 6 MB. A single data center base station is, therefore, shared with a minimum of three PSAPs, and more assuming the 6 MB shared link is not exceeded.

All four cost components of Satellite Connectivity are included in GDIT's proposed solution.

Reuse of Existing Equipment

Please confirm your agreement that, to the extent that the parties agree that existing equipment (such as cabinets) is able to be reused for the deployment, a price reduction will be negotiated by the parties.

GDIT confirms our agreement that, to the extent that the parties agree that existing equipment (such as cabinets) is able to be reused for the deployment, a price reduction will be negotiated by the parties.

Additional Services

GDIT's response to section 8.21 Additional Services of the RFR presents EMC VMWare and GDIT University Web-based Learning/Training Solutions. GDIT's cost proposal, however, did not contain pricing for these additional services. Please provide the pricing structure for EMC VMWare and GDIT University Web-based Learning/Training Solutions.

GDIT is providing the following budgetary pricing for the additional services mentioned in response to section 8.21. These prices are to be utilized as budgetary pricing only. Should the Commonwealth wish to utilize one of these additional services, GDIT will engineer the solution to meet the specific requirements of the Commonwealth. The price for the engineering and implementation will be derived from the T&M labor rates proposed.

Additional Service	Frequency	Unit Price	Quantity	Extended Amount
Virtual Web-Based Training				
Virtual Web-Based Training	Non-Recurring	$181,012.11	1	$181,012.11
EMC VMWare Horizon View 5 (VDI)				
Horizon View 5 Hardware & Software w/ Client	Non-Recurring	$628.64	800	$502,912.00
Annual Software Support / Subscription	Recurring	$43,793.86	5	$218,969.30

Forms

Please complete the attached proof of authentication of signature for Terrance Ward.

The Proof of Authentication of Signature form for Terrance Ward has been completed and is attached to this submission.

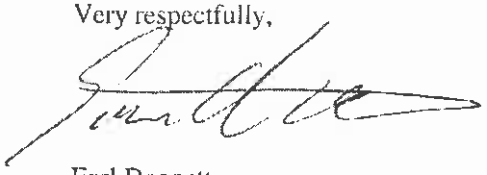
RFR Compliance

Please confirm that wherever the statement "will comply with the RFR specification" appears, GDIT agrees that such response and such statement shall be deemed to state "shall comply with the RFR specification" and shall be considered to mean that GDIT shall comply with the RFR requirement as stated in the RFR or as further clarified in such response.

GDIT confirms that wherever the statement "will" comply with the RFR specification appears in our response, means that GDIT "shall" comply with such RFR requirement.

Following your receipt and review of this letter and the enclosures, if you have any questions or require additional information regarding this submission, please do not hesitate to contact our Contracts Manager at 781-400-7460 or by email at stephen.woodworth@gdit.com.

Very respectfully,



Earl Doggett
Director, Contracts

DUNS Number: 78-580-9349
Vendor ID: 00002829