



Next Generation 9-1-1 Emergency Services Internet Protocol Network

RFP-16-GS-011

Statement of Work

June 24, 2016



Notices

AoE[®], Art of Exploitation[®], AtlasBook[®], BGADrive[®], Connections that Matter[®], Defender9-1-1[®], DopplerNav[®], Enabling Convergent Technologies[®], Galatea[®], GEM9-1-1[®], Geopoke[®], GEM 9-1-1[®], Gokivo[®], Impact[®], Livewire9-1-1[®], Loctronix[®], MO Chat[®], Mond[®], NAVBuilder[®], PerformanScore[®], Proteus[®], Rave9-1-1[®], SwiftLink[®], TCS VoIP Verify[®], The Art of Where[®], TotalCom[®], TrafficBuilder[®], Triton[®], VirtuMedix[®], VoIP Verify[®], Xypoint[®], and Workforce Locator[®] are registered trademarks, and Cyber9-1-1[™], DopplerNav[™], EMedia[™], Emergency Communications Evolved[™], EMInet[™], GeoNexus[™], Intrepid9-1-1[™], Jax9-1-1[™], Locating Anything, Everywhere[™], Look & Design[™], Look4[™], Lynx[™], M8[™], TCS Deployable Communications[™], TCS Family Locator[™], TCS NavTel[™], TCS Ultra[™], Trusted Circle[™], VoLTE9-1-1[™], and WinWhere[™] are trademarks of TCS in the U.S. and certain other countries.

All other brand names and product names used in this document are trademarks, registered trademarks, or service marks of their respective holders.

TCS currently holds more than 400 issued patents and has more than 300 patent applications pending worldwide. Its patents cover a broad spectrum of technologies, including wireless data, text and voice telecommunications, location-based services, GIS/mapping, intercarrier messaging, secure communications, public safety/E9-1-1, and mobile navigation.

Nasdaq GS: CMTL



Table of Contents

- 1. Introduction..... 1**
- 1.1. Intentionally Omitted..... 1**
- 2. Solution Overview 2**
- 2.1. Data Centers and Trunk Aggregation Locations 2**
- 2.1.1. *Data Centers and Trunk Aggregation Locations Description 2*
- 2.1.2. *Data Centers and Trunk Aggregation Locations Proposal References 2*
- 2.2. Next Generation Core Services 3**
- 2.2.1. *Legacy Selective Router Gateway/Protocol Interworking Function..... 4*
- 2.2.2. *Legacy Network/Selective Router Gateway/Protocol Interworking Function..... 5*
- 2.2.3. *Legacy Selective Router Gateway – Legacy Network Gateway/ NG9-1-1 Specific Interworking Function..... 8*
- 2.2.4. *Legacy Network Gateway/Location Interworking Function..... 9*
- 2.2.5. *Legacy PSAP Gateway – RFAI/Location Interworking Function and NG9-1-1 Specific Interworking Function..... 11*
- 2.2.6. *Legacy PSAP Gateway/Protocol Interworking Function 13*
- 2.2.7. *Direct SIP i3 Connection to PSAPs (NENA i3) 18*
- 2.2.8. *Emergency Services Routing Proxy 20*
- 2.2.9. *Policy Routing Function..... 21*
- 2.2.10. *Spatial Information Function..... 23*
- 2.2.11. *Emergency Call Routing Function (ECRF) 29*
- 2.2.12. *Location Validation Function 32*
- 2.2.13. *Media Server 33*
- 2.2.14. *Border Control Function..... 34*
- 2.2.15. *Network LIS..... 35*
- 2.3. Other Provided Services 39**
- 2.3.1. *Logging..... 39*
- 2.3.2. *Reporting..... 42*
- 2.3.3. *Statewide GIS Database..... 45*
- 2.3.4. *Data Provisioning 48*
- 2.3.5. *Multimedia 49*
- 2.3.6. *Documentation 50*



2.4. Operational Considerations 51

 2.4.1. *General Operations*..... 51

 2.4.2. *Availability* 52

 2.4.3. *Performance*..... 54

 2.4.4. *Hardware Compliance* 54

 2.4.5. *System and Network Monitoring*..... 56

 2.4.6. *PSAP Abandonment Process*..... 57

2.5. Security..... 58

 2.5.1. *NENA NG-SEC 75-001 Compliance*..... 58

 2.5.2. *Washington OCIO Policy Compliance* 59

2.6. Standards Compliance..... 60

 2.6.1. *NENA 08-751 Compliance*..... 60

 2.6.2. *NENA i3 [08-003] Compliance*..... 61

2.7. Other Options Selected from the RFP..... 62

 2.7.1. *LNG(s) to ESRP* 62

 2.7.2. *ESRP PSTN Gateway Routing* 63

 2.7.3. *Monitoring Dashboard*..... 63

 2.7.4. *PSTN Gateway* 65

 2.7.5. *Callback Numbers for Failed Calls* 66

 2.7.6. *Callback Number System* 67

3. Network..... 69

3.1. General Networking..... 69

3.2. TCS MPLS Network 70

 3.2.1. *TCS MPLS Network Description* 70

 3.2.2. *TCS MPLS Network Responsibilities* 70

3.3. ESInet MPLS Network 70

 3.3.1. *ESInet MPLS Network Description*..... 70

 3.3.2. *ESInet MPLS Network Responsibilities* 70

 3.3.3. *ESInet MPLS Network Proposal References* 71

3.4. TDM..... 71

 3.4.1. *Voice [12a] TDM* 71

3.5. Media (Voice/Text/Video)..... 72



3.5.1. Voice Services 72

3.5.2. Text Services..... 73

3.5.3. Video Services 74

4. Interconnection 75

4.1. SIP and i3-Compliant CPE Interconnection 75

4.1.1. SIP and i3-Compliant CPE Interconnection Description 75

4.1.2. SIP and i3-Compliant CPE Interconnection Responsibilities 75

4.1.3. SIP and i3-Compliant CPE Interconnection Proposal References..... 75

4.2. Interconnection with ALI Database(s) 75

4.2.1. Interconnection with ALI Databases Description 75

4.2.2. Interconnection with ALI Databases Responsibilities 76

4.3. Interconnection with Dynamic ALI Database(s)..... 76

4.3.1. Interconnection with Dynamic ALI Database(s) Description..... 76

4.3.2. Interconnection with Dynamic ALI Database(s) Responsibilities 76

5. Implementation 78

5.1. Implementation Description..... 78

5.2. Implementation Responsibilities..... 78

5.3. Project Management 79

5.3.1. Implementation Plan 80

5.3.2. Critical Milestones 80

5.3.3. CPE Compatibility Testing..... 80

5.4. Acceptance Test Plan 80

5.5. Implementation Proposal References..... 80

6. Supported Call Flows 82

6.1. Summary of Supported Call Flows 82

6.2. Call Origination via LSRG – ESN Routed 83

6.3. Call Origination via LNG – ESN Routed..... 84

6.4. Call Origination via BCF – ESN Routed 85

6.5. Call Origination via LNG – Location Routed 86

6.6. Call Origination via BCF – Location Routed 87

6.7. Call Transfer from an LPGCAMA PSAP 88

6.8. Call Transfer from an LPGRFAI PSAP 89



6.9.	Call Transfer from an i3 PSAP	90
6.10.	Call Transfer – “Figure 4 Reference” General Conferencing	91
7.	MIL ESInet Requirements	92
7.1.	Global ESInet Requirements [RFP 6.1]	92
7.1.1.	<i>Federal Communications Commission (FCC) Rules – [RFP 6.1.1]</i>	92
7.1.2.	<i>Industry Standards – [RFP 6.1.2]</i>	92
7.1.3.	<i>Support for IPv4 and IPv6 – [RFP 6.1.3]</i>	94
7.1.4.	<i>IP Compliance – [RFP 6.1.4]</i>	95
7.1.5.	<i>SIP Interface Specification – [RFP 6.1.5]</i>	95
7.1.6.	<i>Existing SIP Compatibility – [RFP 6.1.6]</i>	95
7.1.7.	<i>Bandwidth per Audio Session (Call) – [RFP 6.1.7]</i>	96
7.1.8.	<i>Call Quality – [RFP 6.1.8]</i>	96
7.1.9.	<i>Guaranteed Bandwidth (Hard QoS) – [RFP 6.1.9]</i>	96
7.1.10.	<i>Time Changes – [RFP 6.1.10]</i>	96
7.1.11.	<i>No Single Point of Failure – [RFP 6.1.11]</i>	96
7.1.12.	<i>“365 X 24 X 7” ESInet Monitoring System – [RFP 6.1.12]</i>	98
7.1.13.	<i>Automatic Fail-Over – [RFP 6.1.13]</i>	99
7.1.14.	<i>Shared Infrastructure – [RFP 6.1.14]</i>	99
7.1.15.	<i>Outage Notification – [RFP 6.1.15]</i>	107
7.1.16.	<i>Failed Calls Report – [RFP 6.1.16]</i>	108
7.1.17.	<i>Call Back Numbers for Failed Calls – [RFP 6.1.17]</i>	108
7.1.18.	<i>Call Back Number System – [RFP 6.1.18]</i>	109
7.1.19.	<i>Identification of Location of Critical Infra-Structure – [RFP 6.1.20]</i>	111
7.1.20.	<i>Implementation Timeline(s) – [RFP 6.1.21]</i>	111
7.1.21.	<i>Acceptance Test Plan (ATP) – [RFP 6.1.22]</i>	113
7.1.22.	<i>Trouble Escalation Procedures – [RFP 6.1.23]</i>	138
7.1.23.	<i>Outage Notification Process – [RFP 6.1.24]</i>	138
7.1.24.	<i>System Documentation – [RFP 6.1.25]</i>	141
7.2.	ESInet (Core) Requirements [RFP 6.2]	144
7.2.1.	<i>ESInet Infrastructure – [RFP 6.2.1]</i>	145
7.2.2.	<i>Network Location Information Service (NLIS) – [RFP 6.2.2]</i>	146



7.2.3.	<i>Legacy Network Gateway (LNG) Originating Network Interconnection – [RFP</i>	
6.2.3]	<i>148</i>	
7.2.4.	<i>BCF – [RFP 6.2.4].....</i>	<i>152</i>
7.2.5.	<i>ESRP – [RFP 6.2.5].....</i>	<i>157</i>
7.2.6.	<i>PRF [RFP 6.2.6].....</i>	<i>164</i>
7.2.7.	<i>PRF Policy Rules Store [RFP 6.2.7].....</i>	<i>167</i>
7.2.8.	<i>ECRF [RFP 6.2.8].....</i>	<i>170</i>
7.2.9.	<i>Location Validation Function (LVF) – [RFP 6.2.9].....</i>	<i>180</i>
7.2.10.	<i>PSTN Gateway(s) – [RFP 6.2.10].....</i>	<i>182</i>
7.2.11.	<i>Statewide GIS Database – [RFP 6.2.11].....</i>	<i>182</i>
7.2.12.	<i>Spatial Information Function (SIF) – [RFP 6.2.12].....</i>	<i>189</i>
7.2.13.	<i>Security [RFP 6.2.13].....</i>	<i>195</i>
7.2.14.	<i>Basic Call Processing – [RFP 6.2.14].....</i>	<i>201</i>
7.2.15.	<i>Basic Call Processing Enhancements [RFP 6.2.15].....</i>	<i>234</i>
7.2.16.	<i>INTENTIONALLY OMITTED.....</i>	<i>235</i>
7.2.17.	<i>INTENTIONALLY OMITTED.....</i>	<i>235</i>
7.2.18.	<i>ESInet Support for Legacy (CAMA) PSAPs – Legacy PSAP Gateway [RFP</i>	
6.2.18]	<i>235</i>	
7.2.19.	<i>ESInet Connectivity – [RFP 6.2.19].....</i>	<i>236</i>
7.2.20.	<i>INTENTIONALLY OMITTED.....</i>	<i>236</i>
7.2.21.	<i>Logging and Reporting Functions [RFP 6.2.21].....</i>	<i>236</i>
7.2.22.	<i>Monitoring Dashboard – [RFP 6.2.22].....</i>	<i>240</i>
7.3.	Support for Multi-Node PSAPs [RFP 6.3].....	240
7.3.1.	<i>Multi-Node: Host-to-Host Connectivity – [RFP 6.3.1].....</i>	<i>241</i>
7.4.	Facilitating Carrier Transition – [RFP 6.4].....	241
7.4.1.	<i>Conversion of Legacy (CAMA) PSAPs – [RFP 6.4.1].....</i>	<i>256</i>
7.4.2.	<i>Direct IP-Connected PSAPs – [RFP 6.4.2].....</i>	<i>256</i>



List of Exhibits

Exhibit 1. Solution Overview	2
Exhibit 2. Data Centers and Trunk Aggregation Locations Proposal References	3
Exhibit 3. NGCS Proposal References	3
Exhibit 4. LSRG/PIF and Networking.....	4
Exhibit 5. LSRG/PIF Service Responsibility Table	5
Exhibit 6. LSRG/PIF Ingress Methods Supported	5
Exhibit 7. LNG/PIF and Networking.....	6
Exhibit 8. LNG/PIF and Networking Responsibilities	6
Exhibit 9. LNG/PIF Ingress Methods Supported	7
Exhibit 10. LNG/PIF Proposal References	7
Exhibit 11. LNG-LSRG/NIF to ESRP/PRF.....	8
Exhibit 12. LNG/PIF and Networking Responsibilities	8
Exhibit 13. LNG/LIF to ALI for Location.....	9
Exhibit 14. LNG/LIF Responsibilities.....	9
Exhibit 15. LNG/LIF Connectivity and Interface Method	10
Exhibit 16. LNG/LIF Proposal References.....	10
Exhibit 17. RFAI Networking.....	11
Exhibit 18. LPGRFAI/NIF Responsibilities	11
Exhibit 19. LPGRFAI-Connected PSAPs.....	12
Exhibit 20. LPGRFAI/NIF Proposal References	13
Exhibit 21. LPG/PIF and Networking	14
Exhibit 22. LPG/PIF Responsibilities	15
Exhibit 23. CAMA-LPG/PIF-Connected PSAPs	15
Exhibit 24. CAMA-LPG/PIF Proposal References.....	18
Exhibit 25. Direct SIP (i3) Networking.....	18
Exhibit 26. Direct SIP i3 Connection Responsibilities.....	19
Exhibit 27. Direct SIP i3-Connected PSAPs.....	19
Exhibit 28. Direct Connected i3 Proposal References	20
Exhibit 29. Direct SIP i3 Connection Responsibilities.....	20
Exhibit 30. [12a] Routing Methods	21
Exhibit 31. ESRP Proposal References	21



Exhibit 32. [12a] Routing Methods 21

Exhibit 33. PRF Responsibilities 22

Exhibit 34. PRF Proposal References 23

Exhibit 35. GIS Data Layers and Quality Control Processes 27

Exhibit 36. SIF Responsibilities 28

Exhibit 37. SIF Proposal References 29

Exhibit 38. ECRF Responsibilities 31

Exhibit 39. ECRF Proposal References 31

Exhibit 40. [12a] Spatial Router LVF Training 32

Exhibit 41. LVF Training Topics 32

Exhibit 42. LVF Responsibilities 32

Exhibit 43. LVF Proposal References 33

Exhibit 44. Media Server Methods and PSAP CPE Supported 33

Exhibit 45. Media Server Responsibilities 33

Exhibit 46. BCF Codec Table 34

Exhibit 47. BCF Responsibilities 35

Exhibit 48. BCF Proposal References 35

Exhibit 49. DBMS Capabilities 36

Exhibit 50. Data Management Commitments for NLIS 37

Exhibit 51. NLIS Responsibilities 38

Exhibit 52. NLIS Proposal References 39

Exhibit 53. Logging Responsibilities 41

Exhibit 54. Logging Proposal References 42

Exhibit 55. Reporting Responsibilities 44

Exhibit 56. Reporting Proposal References 44

Exhibit 57. Statewide GIS Database Responsibilities 47

Exhibit 58. Statewide GIS Database Proposal References 48

Exhibit 59. Data Provisioning Responsibilities 49

Exhibit 60. Multimedia Responsibilities 49

Exhibit 61. Multimedia Proposal References 50

Exhibit 62. Documentation Responsibilities 51

Exhibit 63. Documentation Proposal References 51



Exhibit 64. General Operations Responsibilities	52
Exhibit 65. General Operations Proposal References	52
Exhibit 66. Availability Responsibilities	53
Exhibit 67. Availability Proposal References	53
Exhibit 68. Performance Responsibilities	54
Exhibit 69. Performance Proposal References	54
Exhibit 70. Hardware Compliance Responsibilities	56
Exhibit 71. Hardware Compliance Proposal References	56
Exhibit 72. System and Network Monitoring Responsibilities	56
Exhibit 73. Monitoring Proposal References.....	57
Exhibit 74. PSAP Abandonment Responsibilities.....	58
Exhibit 75. PSAP Abandonment Proposal References.....	58
Exhibit 76. NENA NG-SEC 75-001 Compliance Responsibilities.....	59
Exhibit 77. NENA NG-SEC 75-001 Proposal References	59
Exhibit 78. Washington OCIO Policy Compliance Responsibilities	59
Exhibit 79. Washington OCIO Policy Compliance Proposal References	60
Exhibit 80. Standards Compliance Proposal References	60
Exhibit 81. NENA 08-751 Compliance Responsibilities	60
Exhibit 82. NENA 08-751 Compliance Proposal References	61
Exhibit 83. NENA i3 [08-003] Compliance Responsibilities	61
Exhibit 84. NENA i3 [08-003] Compliance Proposal References	61
Exhibit 85. LNG(s) to ESRP Responsibilities.....	62
Exhibit 86. LNG(s) to ESRP Proposal References.....	62
Exhibit 87. LNG(s) to ESRP Responsibilities.....	63
Exhibit 88. ESRP PSTN Proposal References.....	63
Exhibit 89. Monitoring Dashboard Responsibilities.....	64
Exhibit 90. Monitoring Dashboard Proposal References.....	65
Exhibit 91. PSTN Gateway Responsibilities.....	65
Exhibit 92. PSTN Gateway Proposal References.....	66
Exhibit 93. Call Back Numbers for Failed Calls Responsibilities	66
Exhibit 94. Call-Back Numbers for Failed Calls Proposal References.....	67
Exhibit 95. Callback Number System Responsibilities	67



Exhibit 96. Call-Back Number System Proposal References.....	68
Exhibit 97. General Networking Responsibilities	69
Exhibit 98. General Networking Proposal References	69
Exhibit 99. TCS MPLS Network Responsibilities	70
Exhibit 100. ESInet MPLS Network Responsibilities	71
Exhibit 101. ESInet MPLS Proposal References	71
Exhibit 102. Voice [12a] Responsibilities.....	71
Exhibit 103. TDM Proposal References.....	72
Exhibit 104. Voice Services Responsibilities.....	72
Exhibit 105. Text Services Responsibilities	73
Exhibit 106. Text Services Proposal References	74
Exhibit 107. Video Services Responsibilities	74
Exhibit 108. Video Services Proposal References	74
Exhibit 109. SIP and i3-Compliant CPE Interconnection Responsibilities.....	75
Exhibit 110. Video Services Proposal References	75
Exhibit 111. Interconnection with ALI Databases Responsibilities	76
Exhibit 112. Interconnection with Dynamic ALI Database(s) Responsibilities	76
Exhibit 113. Implementation Responsibilities.....	78
Exhibit 114. Implementation Proposal References.....	80
Exhibit 115. Omitted.....	81
Exhibit 116. Call Origination via LSRG – ESN Routed.....	83
Exhibit 117. Call Origination via LNG – ESN Routed.....	84
Exhibit 118. Call Origination via BCF – ESN Routed	85
Exhibit 119. Call Origination via LNG – Location Routed	86
Exhibit 120. Call Origination via BCF – Location Routed	87
Exhibit 121. Call Transfer from an LPGCAMA PSAP	88
Exhibit 122. Call Transfer from an LPGRFAI PSAP	89
Exhibit 123. Call Transfer from an i3 PSAP	90
Exhibit 124. Call Transfer – “Figure 4 Reference” General Conferencing	92
Exhibit 125. TCS Network Operations Center	98
Exhibit 126. Express IBOP Screenshot.....	101
Exhibit 127. IBOP Process Diagram	102



Exhibit 128. Blank IBOP Template.....	103
Exhibit 129. Blank IBOP Template for Pre-implementation NOC Information.....	104
Exhibit 130. Blank IBOP Template for Implementation Information	105
Exhibit 131. Blank IBOP Template for Approval Signatures	106
Exhibit 132. NOC Event Notification Process.....	108
Exhibit 133. On-the-Fly Polygon Creation	110
Exhibit 134. [12a] ESInet Implementation Schedule	112
Exhibit 135. Escalation Resources.....	138
Exhibit 136. NOC Event Notification Process.....	139
Exhibit 137. SIL Table.....	140
Exhibit 138. High-Level View of TCS Hosted NG9-1-1 Architecture	142
Exhibit 139. Table of Contents from TCS' Established Disaster Recovery Plan	143
Exhibit 140. Logical Call Flow Documentation for Text-to-911.....	144
Exhibit 141. Call Flow Diagram	149
Exhibit 142. Texting Solution Overview	155
Exhibit 143. [12a] Features	161
Exhibit 144. ECRF and LVF Architecture.....	163
Exhibit 145. PRF Time of Day Example Rule.....	167
Exhibit 146. [12a] User Adds Time of Day Rule.....	168
Exhibit 147. [12a] Confirmation Screen	168
Exhibit 148. [12a] Summary View of Transaction Logs	168
Exhibit 149. New Time of Day Rule Being Created on [12a].....	169
Exhibit 150. Policy Routing Function Portal.....	170
Exhibit 151. [12a] Spatial Router	181
Exhibit 152. [12a] Spatial Router (LVF).....	182
Exhibit 153. [12a] Products and Services.....	189
Exhibit 154. SLAs, Metrics, and Limitations	191
Exhibit 155. Manual Quality Control Processes	193
Exhibit 156. Data Points Contained in [12a] Quarterly Reports.....	194
Exhibit 157. NENA NG-SEC 75-001 Compliance.....	195
Exhibit 158. Washington OCIO Policy Compliance.....	198
Exhibit 159. Basic Call Processing Compliance Matrix.....	201



Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AC	Alternating Current
AJAX	Asynchronous JavaScript and XML
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AoR	Address of Record
AP	Access Point
APCO	Association of Public-Safety Communications Officials
AQPS	ALI Quality Process Services
ATAC	Advanced Technical Assistance Center
ATIS	Alliance for Telecommunications Industry Solutions
ATP	ACCEPTANCE TEST PLAN
AVL	Automatic Vehicle Location
B2BUA	Back-to-Back User Agent
BCF	Border Control Function
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
CAD	Computer-Aided Dispatch
CAMA	Centralized Automatic Message Accounting
CBN	Callback Number
CDR	Call Detail Record
CE	Conformité Européene
CIDB	Call Information Database
CIG	Cyber Intelligence Group
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CJIS	Criminal Justice Information Services
CLC	Call Logic Center
CLEC	Competitive Local Exchange Carrier
COID	Company ID
COTS	Commercial Off-the-Shelf
CPE	Customer Premises Equipment
CPN	Calling Party Number

Acronym	Definition
cps	Calls Per Second
CSA	Canadian Standards Association
CSEC	Commission on State Emergency Communications
CSP	Communications Service Provider
CSRIC	Communications Security, Reliability and Interoperability Council
CVSS	Common Vulnerability Scoring System
DBMS	Database Management System
DC	Direct Current
DEM	Digital Evidence Management
DoD	Department of Defense
DoS	Denial of Service
DTMF	Dual Tone Multifrequency
E9-1-1	Enhanced 9-1-1
ECaTS	Emergency Call Tracking System
ECD	Emergency Communications District
ECRF	Emergency Call Routing Function
ECRIT	Emergency Context Resolution with Internet Technologies
EENA	European Emergency Number Association
EGDMS	Enterprise Geodatabase Management System
EIA	Electronic Industries Alliance
ELT	English Language Translation
E-MF	Enhanced Multifrequency
EMI	Electromagnetic Interference
E-PRF	Enhanced Policy Routing Function
ESA	Emergency Service Agency
ESIF	Emergency Services Interconnection Forum
ESInet	Emergency Services IP Network
ESN	Emergency Service Number
ESP	Enterprise Security and Protection
ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Proxy
ESZ	Emergency Services Zone
ETL	Extract/Transform/Load
FBI	Federal Bureau of Investigation



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

Acronym	Definition
FCC	Federal Communications Commission
FTP	File Transfer Protocol
GIS	Geographic Information System
GMLC	Gateway Mobile Location Center
GUI	Graphical User Interface
HELD	HTTP-Enabled Location Delivery
HIPAA	Health Insurance Portability and Accountability Act
HSEMD	Homeland Security and Emergency Management Department
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBOP	Implementation and Back-Out Plan
ICE	Industry Collaboration Event
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IOT	Interoperability Testing
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
ISDN	Integrated Services Digital Network
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISUP	ISDN User Part
LAN	Local Area Network
LATA	Local Access and Transport Area
lat/lon	Latitude/Longitude
LBS	Location-Based Services
LbyR	Location by Reference
LbyV	Location by Value
LDB	Location Database
LIF	Location Interworking Function
LIS	Location Information Server

Acronym	Definition
LMR	Land Mobile Radio
LNG	Legacy Network Gateway
LoST	Location to Service Translation
LPG	Legacy PSAP Gateway
LPGRFAI	Legacy PSAP Gateway – RFAI
LSRG	Legacy Selective Router Gateway
LVF	Location Validation Function
M3UA	MTP3 User Adaptation
MF	Multifrequency
MIL	Washington State Military Department
MIS	Management Information System
MOS	Mean Opinion Score
MPC	Mobile Positioning Center
MPLS	Multi-Protocol Label Switching
MSAG	Master Street Address Guide
MSRP	Message Session Relay Protocol
NAT	Network Address Translation
NCCIC	National Cybersecurity and Communications Integration Center
NCTCOG	North Central Texas Council of Governments
NENA	National Emergency Number Association
NetTN	Network Tennessee
NG9-1-1	Next Generation 9-1-1
NGCS	Next Generation Core Services
NIF	NG9-1-1–Specific Interworking Function
NLIS	Network Location Information Service
NOC	Network Operations Center
NPA	Numbering Plan Area
NRF	No Record Found
OCIO	Office of the Chief Information Officer
OGC	Open Geospatial Consortium
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
OSP	Originating Service Provider
OTF	On the Fly
OWASP	Open Web Application Security Project
P25	Project 25
P2P	Peer to Peer



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

Acronym	Definition
pANI	Pseudo Automatic Number Identification
PBX	Private Branch Exchange
PIDF-LO	Presence Information Data Format – Location Object
PIF	Protocol Interworking Function
PM	Program Manager
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Professional
PM WIN-T	Project Manager Warfighter Information Network – Tactical
PNL	Preferred Network List
POC	Point of Contact
POP	Point of Presence
POTS	Plain Old Telephone Service
PPM	Project Portfolio Management
PRF	Policy Routing Function
PRI	Primary Rate Interface
PRR	Policy Routing Rule
PSAP	Public Safety Answering Point
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
PTZ	Pacific Time Zone
QA	Quality Assurance
QC	Quality Control
QoS	Quality of Service
RCA	Root Cause Analysis
RFAI	Request for Assistance Interface
RFC	Request for Comment
RFP	Request for Proposal
RMS	Routing Management Service
RPC	Regional Planning Commission
RTP	Real-Time Transfer Protocol
SaaS	Software as a Service
SBC	Session Border Controller
SDE	Spatial Database Engine
SDO	Standards Development Organization
SFTP	Secure File Transfer Protocol
SI	Spatial Interface

Acronym	Definition
SIF	Spatial Information Function
SIL	Service Impairment Level
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOC	Service Organization Control
SOI	Service Order Input
SONET	Synchronous Optical Network
SOW	Statement of Work
SR	Selective Router
SS7	Signaling System 7
SSG	Safety and Security Group
STP	Signal Transfer Point
TCC	Text Control Center
TCP	Transmission Control Protocol
TCS	TeleCommunication Systems, Inc.
TDM	Time-Division Multiplexing
TECB	Tennessee Emergency Communications Board
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TOPS	Technical Operations
TTY	Teletypewriter
UBI	Uniform Business Identification
UDP	User Datagram Protocol
UI	User Interface
UL	Underwriters Laboratories
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Universal Coordinated Time
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
W3C	World Wide Web Consortium



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

Acronym	Definition
WACIRC	Washington Computer Incident Response Center
WAN	Wide Area Network
WEP	Wired Equivalent Privacy

Acronym	Definition
WFS	Web Feature Service
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II



1. Introduction

1.1. Intentionally Omitted



2. Solution Overview

2.1. Data Centers and Trunk Aggregation Locations

2.1.1. Data Centers and Trunk Aggregation Locations Description

The TCS data centers for the service delivery for this SOW [12a]
[12a]

The trunk aggregation locations for this project will be determined in the initial phases of the project.

Exhibit 1 shows a diagram of the overall system solution.

[12a]



Exhibit 1. Solution Overview

2.1.2. Data Centers and Trunk Aggregation Locations Proposal References

Exhibit 2 lists the applicable proposal and request for proposal (RFP) references.



Exhibit 2. Data Centers and Trunk Aggregation Locations Proposal References

Proposal Section #	Proposal Section Title
11.1.19	Identification of Location of Critical Infra-Structure – [RFP 6.1.20]

2.2. Next Generation Core Services

This is the list of Next Generation Core Services (NGCS) TCS will use to provide Next Generation 9-1-1 (NG9-1-1) managed services associated with this SOW.

Transitory Services

- Legacy Selective Router Gateway (LSRG)/Protocol Interworking Function (PIF) and NG9-1-1 Specific Interworking Function (NIF)
- Legacy Network Gateway (LNG)/PIF, NIF, and Location Interworking Function (LIF)
- Legacy PSAP Gateway (LPG)/ PIF, NIF, and Location Interworking Function (LIF)
- LPGRFAI/NIF – LPG/NIF for Request for Assistance Interface (RFAI) interconnected Customer Premises Equipment (CPE) (software only) – This is a customization for the Alliance for Telecommunications Industry Solutions (ATIS) RFAI standard as required for **[12a]** CPE integration.

End-State Services

- Emergency Services Routing Proxy (ESRP)/Policy Routing Function (PRF)
- Spatial Information Function (SIF)
- Emergency Call Routing Function (ECRF)
- Location Validation Function (LVF)
- Direct Session Initiation Protocol (SIP) i3 from the ESRP to National Emergency Number Association (NENA) i3-compliant Public Safety Answering Points (PSAPs)
- Media Server – The Media Server manages voice mixing for the purpose of bridging and conferencing 9-1-1 calls
- Border Control Function (BCF)
- Network Location Information Server (LIS), starting with legacy Automatic Location Identification (ALI)

Sections 2.2.1 through 2.2.15 provide details about each of these services.

Exhibit 3 lists the applicable proposal and RFP references for overall NGCS.

Exhibit 3. NGCS Proposal References

Proposal Section #	Proposal Section Title
11.2	ESInet (Core) Requirements [RFP 6.2]
11.2.1	ESInet Infrastructure – [RFP 6.2.1]



2.2.1. Legacy Selective Router Gateway/Protocol Interworking Function

2.2.1.1. LSRG/PIF Description

The LSRG/PIF connects with selective routers (SRs).

[12a]

[Redacted text block]

[12a]

[Large redacted area]

Exhibit 4. LSRG/PIF and Networking



2.2.1.2. LSRG/PIF Responsibilities

Exhibit 5 delineates responsibilities between TCS and MIL for the LSRG/PIF.

Exhibit 5. LSRG/PIF Service Responsibility Table

Reference #	System/Service	Responsibility	
		TCS	MIL
LSRGPIF-01	LSRG/PIF available to connect to SRs	R	
LSRGPIF-02	Circuit connectivity to/from the LSRG/PIF and SRs	R	
LSRGPIF-03	MPLS connectivity available for the LSRG/PIF to ISUP/SIP gateway	R	
LSRGPIF-04	LSRG/PIF configured with appropriate data to enable call delivery for supported call flows	R	
LSRGPIF-05	LSRG/PIF connected to TCS' Multi-Protocol Label Switching (MPLS) network for monitoring and management	R	
LSRGPIF-06	Provide list of all SRs required for this project		R
LSRGPIF-07	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

[12a]

Exhibit 6 shows the supported ingress methods for LSRG/PIF.

Exhibit 6. LSRG/PIF Ingress Methods Supported

Ingress Methods Supported	Description
Main Ingress Methods:	
[12] TDM	[12a]
Alternate Ingress Methods:	
Multifrequency (MF)	MF TDM trunks
Enhanced Multifrequency (E-MF)	E-MF trunks (like Feature Group-D)

[12a]

2.2.2. Legacy Network/Selective Router Gateway/Protocol Interworking Function

2.2.2.1. LNG/PIF Description

The LNG/PIF connects with Communications Service Providers (CSPs) using TDM ingress.



[12a]

[Redacted text block]

[12a]

[Large redacted text block]

Exhibit 7. LNG/PIF and Networking

2.2.2.2. LNG/PIF Responsibilities

Exhibit 8 delineates responsibilities between TCS, MIL, and CSPs for LNG/PIF and networking.

Exhibit 8. LNG/PIF and Networking Responsibilities

Reference #	System/Service	Responsibility		
		TCS	MIL	CSPs
LNGPIF-01	LNG/PIF available to connect to CSPs	R		



Reference #	System/Service	Responsibility		
		TCS	MIL	CSPs
LNGPIF-02	Circuit connectivity to/from the originating service providers	C		R
LNGPIF-03	Issue Network Notification	I	R	
LNGPIF-04	Schedule cutover of CSP circuits (for each CSP)	R		I
LNGPIF-05	Test CSP circuits prior to cutover	R		I
LNGPIF-06	Cut-over circuits	R		I
LNGPIF-07	Decommission old trunks and update records	I		R
LNGPIF-08	MPLS connectivity available for the LNG/PIF to ISUP/SIP gateway	R		
LNGPIF-09	LNG/PIF configured with appropriate data to enable call delivery for supported call flows	R		
LNGPIF-10	LNG/PIF connected to TCS MPLS network for monitoring and management	R		
LNGPIF-11	Provide list of originating service providers for this project		R	
LNGPIF-12	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R	

Legend: "R" Responsible, "I" Informed, "C" Consulted

[12a]

Exhibit 9 shows the supported ingress methods for LNG/PIF.

Exhibit 9. LNG/PIF Ingress Methods Supported

Ingress Methods Supported	Description
Main Ingress Methods:	
ISUP [12]	[12a]
Alternate Ingress Methods:	
MF	MF TDM trunks
E-MF	E-MF trunks (Like Feature Group-D)

[12a]

2.2.2.3. LNG/PIF Proposal References

Exhibit 10 lists the applicable proposal and RFP references for LNG/PIF.

Exhibit 10. LNG/PIF Proposal References

Proposal Section #	Proposal Section Title
7.2.3	Legacy Network Gateway (LNG) Originating Network Interconnection – [RFP 6.2.3]



Proposal Section #	Proposal Section Title
7.2.3.2	SIP Conversion – [RFP 6.2.3.2]
7.2.3.3	Audio CODEC – [RFP 6.2.3.3]

2.2.3. Legacy Selective Router Gateway – Legacy Network Gateway/ NG9-1-1 Specific Interworking Function

2.2.3.1. LNG-LSRG/NIF Description

[Redacted text block]

[Redacted text block]

Exhibit 11. LNG-LSRG/NIF to ESRP/PRF

2.2.3.2. LNG-LSRG/NIF Responsibilities

Exhibit 12 delineates responsibilities between TCS and MIL for [Redacted] services.

Exhibit 12. LNG/PIF and Networking Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LNGNIF-01	MPLS network available for the [Redacted] to reach [Redacted] and PSAPs	R	
LNGNIF-02	[Redacted] of SIP signaling with [Redacted]	R	
LNGNIF-03	BCF configured to allow traffic from [Redacted] to the [Redacted]	R	
LNGNIF-04	[Redacted] of receiving and sending call-related messaging and voice to PSAPs	R	
LNGNIF-05	Accurate and timely trouble reporting and description of problems to TCS [Redacted], for events where TCS has no visibility, per established reporting procedures		R



Legend: “R” Responsible, “I” Informed, “C” Consulted

2.2.4. Legacy Network Gateway/Location Interworking Function

2.2.4.1. LNG/LIF Description

The LNG LIF service provides connectivity to ALI database pairs, LIS, and dynamic ALIs like Mobile Positioning Centers (MPCs)/VoIP Positioning Centers (VPCs)/Gateway Mobile Location Centers (GMLCs). ALI is queried using the NENA 04-001 messaging standard and inserts that data into the Presence Information Data Format – Location Object (PIDF-LO) for wireline and Voice over Internet Protocol (VoIP) i2 calls, or a Location by Reference (LbyR) for wireless for transmission to the ESRP/PRF. [12a]

[Redacted]

Exhibit 13 shows the general connectivity model for the LNG/LIF.



Exhibit 13. LNG/LIF to ALI for Location

2.2.4.2. LNG/LIF Responsibilities

Exhibit 14 delineates responsibilities between TCS and MIL for LNG-LSRG/NIF services.

Exhibit 14. LNG/LIF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LNLIF-01	MPLS network available for the LNG/LIF to reach ALIs	R	
LNLIF-02	LNG/LIF available to connect to external location database(s)	R	
LNLIF-03	LNG/LIF connected to ALIs	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
LNGLIF-04	LNG/LIF connected to MPCs/GMLCs/VPCs	R	
LNGLIF-05	LNG/LIF configured and provisioned to send/receive NENA 04-001 queries to the ALI(s)	R	
LNGLIF-06	LNG/LIF configured and provisioned to send/receive [12a] to MPCs/GMLCs/VPCs	R	
LNGLIF-07	Provide authorization to existing ALI providers for TCS to gain connection and service for the execution of this SOW		R
LNGLIF-08	MPLS network available for the LNG/LIF to reach ALIs	R	

Legend: "R" Responsible, "I" Informed, "C" Consulted

[12a]

[Redacted text block]

Exhibit 15 shows the LNG/LIF connectivity and corresponding interface method.

Exhibit 15. LNG/LIF Connectivity and Interface Method

LIF Connectivity	LIF Method/Interface
ALI (for wireline) – NLIS	NENA 04-001
MPC/GMLC (for wireless)	[12]
VPC (for VoIP)	[12]

2.2.4.3. LNG/LIF Proposal References

Exhibit 16 lists the applicable proposal and RFP references for LNG/LIF.

Exhibit 16. LNG/LIF Proposal References

Proposal Section #	Proposal Section Title
7.2.3.6	LNG/LIF Location Determination – [RFP 6.2.3.6]
7.2.5.3	Dereferencing – [RFP 6.2.5.3]
7.2.5.4	HELD – [RFP 6.2.5.4]
7.2.18.3	ALI Interface – [RFP 6.2.18.3]



2.2.5. Legacy PSAP Gateway – RFAI/Location Interworking Function and NG9-1-1 Specific Interworking Function

2.2.5.1. LPGRFAI/NIF Description

[12a]

[Redacted text]

Exhibit 17 shows the RFAI networking diagram.



Exhibit 17. RFAI Networking

2.2.5.2. LPGRFAI/NIF Responsibilities

Exhibit 18 delineates responsibilities between TCS and MIL for LPGRFAI/NIF services.

Exhibit 18. LPGRFAI/NIF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LPGRFAI-01	MPLS network available for the LPGRFAI to reach ESRP and PSAPs	R	
LPGRFAI-02	LPGRFAI available to connect to ESRP and PSAPs	R	
LPGRFAI-03	LPGRFAI connected to ESRP	R	
LPGRFAI-04	LPGRFAI configured with appropriate data to enable call delivery	R	
LPGRFAI-05	LPGRFAI capable of receiving and sending call-related messaging	R	
LPGRFAI-06	Provide a list of all [12a] based PSAPs for this project		R
LPGRFAI-07	Provide assistance in the effort to collect "*" codes and other transfer requirements		R
LPGRFAI-08	Accurate and timely trouble reporting and description of problems to TCS [12a] [Redacted], for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted



[12a]

[Redacted text block]

Exhibit 19 lists the LPGRFAI-connected PSAPs.

Exhibit 19. LPGRFAI-Connected PSAPs

PSAP	County	CPE & Version	Redundancy
[12a]	[Redacted]	Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado VIPER	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado, Viper, SIP	Redundant where the CPE supports TCS' [12a] network design
[12a]	[Redacted]	Intrado VIPER (SIP) - [12a]	Redundant where the CPE supports TCS' [12a] network design



		[12a]	
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design
[12a]		Intrado VIPER (SIP)	Redundant where the CPE supports TCS' [12a] network design

2.2.5.3. LPGRFAI/NIF Proposal References

Exhibit 20 lists the applicable proposal and RFP references for LPGRFAI/NIF.

Exhibit 20. LPGRFAI/NIF Proposal References

Proposal Section #	Proposal Section Title
7.2.5.7	Sessions Originating from PSAP – [RFP 6.2.5.7]
7.2.18.4	Support for Star Codes – [RFP 6.2.18.4]
7.4.2	Direct IP-Connected PSAPs – [RFP 6.4.2]

2.2.6. Legacy PSAP Gateway/Protocol Interworking Function

2.2.6.1. LPG/PIF Description

The LPG/PIF service is a NENA standard core service. The LPG/PIF connects NENA i3-compliant SIP signaling to IP-based PSAPs [12a]

Exhibit 21 shows the LPG/PIF and networking diagram.



[12a]

Exhibit 21. LPG/PIF and Networking

NENA i3-compliant LPG/PIFs will be deployed at the PSAPs requiring Centralized Automatic Message Accounting (CAMA) connectivity to their CPE. The LPG/PIFs are connected to the ESInet to facilitate initial call delivery and call transfers, as well as ALI transactions. [12a]

[Redacted]

[Redacted] All these ESInet transactions are facilitated by the LPG (NIF and LIF, respectively) on behalf of the legacy PSAP. They also offer functions that help the PSAP retrieve ALI information – [12a]

[Redacted] – to facilitate both inter- and intra-ESInet call transfers.

TCS' LPG supports a SIP interface with the ESInet in compliance with NENA 08-003.

TCS' LPG supports a CAMA interface with the PSAP CPE in compliance with NENA 08-003.

TCS' ALI interface complies with the applicable requirements identified in NENA 08-003.

The solution supports star code speed dials through the ESInet. [12a]

[Redacted]

[Redacted]

[Redacted] The system supports a legacy CAMA PSAP initiating a conference or transfer to a 10- or 11-digit number.

[12a]

[Redacted]

[Redacted]

[Redacted]



2.2.6.2. LPG/PIF Responsibilities

Exhibit 22 delineates responsibilities between TCS and MIL for LPG/PIF services.

Exhibit 22. LPG/PIF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LPGPIF-01	MPLS network available for the LPG/NIF to reach the LPG/PIF at the PSAPs (where required)	R	
LPGPIF-02	LPG/PIF configured with appropriate data to enable call delivery	R	
LPGPIF-03	LPG/PIF capable of receiving and sending call-related messaging	R	
LPGPIF-04	Provide assistance in the effort to collect "*" codes and other transfer requirements		R
LPGPIF-05	Provide a list of all legacy-based PSAPs for this project		R
LPGPIF-06	Accurate and timely trouble reporting and description of problems to TCS ([12a]), for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

Exhibit 23 lists the CAMA-LPG/PIF-connected PSAPs.

Exhibit 23. CAMA-LPG/PIF-Connected PSAPs

PSAP	County	CPE & Version	Redundancy
[12a]	[12a]	Zetron MaxD [12a]	Redundant
[12a]	[12a]	Intrado VIPER (CAMA) [12a]	Redundant
[12a]	[12a]	Intrado VIPER (CAMA)	Redundant
[12a]	[12a]	Intrado VIPER (CAMA)	Redundant
[12a]	[12a]	Intrado VIPER (CAMA)	Redundant
[12a]	[12a]	Intrado VIPER (CAMA)	Redundant
[12a]	[12a]	Intrado VIPER (CAMA)	Redundant
[12a]	[12a]	Zetron, 3200 [12a]	Redundant



Washington State Military Department
 Next Generation 9-1-1 Emergency Services Internet Protocol Network
 Statement of Work | June 24, 2016

[12a]	Plant CML, VESTA, CAMA	Redundant
	Intrado, Viper, CAMA	Redundant
	Intrado, Viper, CAMA	Redundant
	Intrado, Viper, CAMA	Redundant
	Positron, LifeLine, 100	Redundant
	Zetron Max CT [12a] <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div> <div style="background-color: black; height: 15px; width: 100%;"></div>	Redundant
	Zetron 3000	Redundant
	Positron, LifeLine, 100	Redundant
	Positron, LifeLine, 100	Redundant
	unsure	Redundant
	Motorola ECW 911	Redundant
	Positron, LifeLine, 100	Redundant
	Positron, LifeLine, 100	Redundant
	Positron, LifeLine, 100	Redundant
	Positron, LifeLine, 100	Redundant
	Intrado VIPER (CAMA)	Redundant
Intrado VIPER (CAMA)	Redundant	



**Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016**

[12a]	Cassidian VESTA	Redundant
	Solacom GUARDIAN	Redundant
	Intrado VIPER (CAMA)	Redundant
	Positron, LifeLine, 100	Redundant
	Positron, LifeLine, 100	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Intrado VIPER (CAMA)	Redundant
	Positron Power 911 v5.3	Redundant
Lifeline Power911 EOL 2008	Redundant	



2.2.6.3. CAMA-LPG/PIF Proposal References

Exhibit 24 lists the applicable proposal and RFP references for CAMA-LPG/PIF.

Exhibit 24. CAMA-LPG/PIF Proposal References

Proposal Section #	Proposal Section Title
7.2.5.7	Sessions Originating from PSAP – [RFP 6.2.5.7]
7.2.18	ESInet Support for Legacy (CAMA) PSAPs – Legacy PSAP Gateway [RFP 6.2.18]
7.2.18.1	SIP Interface – [RFP 6.2.18.1]
7.2.18.4	Support for Star Codes – [RFP 6.2.18.4]

2.2.7. Direct SIP i3 Connection to PSAPs (NENA i3)

2.2.7.1. Direct SIP i3 Connection to PSAPs Description

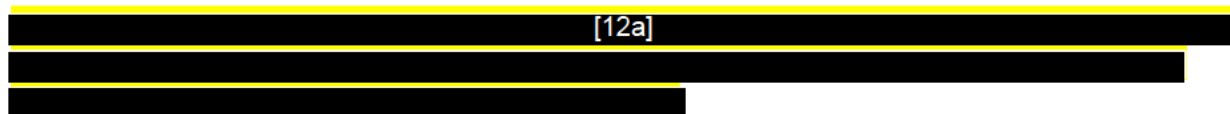
Direct SIP i3 connected PSAPs will receive calls and messages using [12a] as described in the i3 CPE interface specification.

Exhibit 25 shows the direct SIP (i3) networking diagram.



Exhibit 25. Direct SIP (i3) Networking

Direct SIP i3 PSAPs will be deployed on the ESInet to facilitate initial call delivery and call transfers, as well as ALI transactions, from the ESInet.





2.2.7.2. Direct SIP i3 Connection Responsibilities

Exhibit 26 delineates responsibilities between TCS and MIL for direct SIP i3 connection.

Exhibit 26. Direct SIP i3 Connection Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
SIPI3-01	MPLS network available for the ESRP to reach the PSAPs	R	
SIPI3-02	Provide assistance in the effort to collect "*" codes and other transfer requirements		R
SIPI3-03	Provide a list of all NENA i3 based PSAPs for this project		R
SIPI3-04	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED], for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

Exhibit 27 lists the direct SIP i3-connected PSAPs.

Exhibit 27. Direct SIP i3-Connected PSAPs

PSAP	County	CPE & Version	Redundancy
[REDACTED]	[12a]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design
[REDACTED]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design
[REDACTED]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design
[REDACTED]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design
[REDACTED]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design
[REDACTED]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design
[REDACTED]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS [12a] network design



[12a]	[REDACTED]	[REDACTED]	Redundant where the CPE supports TCS' [12a] network design
-------	------------	------------	--

2.2.7.3. Direct Connected i3 Proposal References

Exhibit 28 lists the applicable proposal and RFP references for direct connected i3.

Exhibit 28. Direct Connected i3 Proposal References

Proposal Section #	Proposal Section Title
7.2.5.7	Sessions Originating from PSAP – [RFP 6.2.5.7]
7.3	Support for Multi-Node PSAPs [RFP 6.3]
7.3.1	Multi-Node: Host-to-Host Connectivity – [RFP 6.3.1]
7.4.2	Direct IP-Connected PSAPs – [RFP 6.4.2]

2.2.8. Emergency Services Routing Proxy

2.2.8.1. Emergency Services Routing Proxy Description

The ESRP service provides the signaling interconnection between the LNG-LSRG/NIF, ECRF, LPG/NIF, LPGRFAI/NIF, and LIS [REDACTED] [12a]

2.2.8.2. Emergency Services Routing Proxy Responsibilities

Exhibit 29 delineates responsibilities between TCS and MIL for direct SIP i3 connection.

Exhibit 29. Direct SIP i3 Connection Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
ESRP-01	Ensure ESRP availability to the ESNet	R	
ESRP-02	Provide existing PSAP URIs or assist in the naming scheme	I	R
ESRP-03	Assist and review ESN routing rules per PSAP	I	R
ESRP-04	Assist and review routing methods per PSAP	I	R
ESRP-05	Accurate and timely trouble reporting and description of problems to TCS [REDACTED] [12a] for events where TCS has no visibility, per established reporting procedures	I	R

Legend: “R” Responsible, “I” Informed, “C” Consulted

The ESRP facilitates call routing on behalf of a call ingressing through the LNG/LSRG or BCF. The ESRP coordinates call routing using the [REDACTED] [12a] created by the LNG/LSRG or received at the BCF after receiving a [REDACTED] [12a] response from an ECRF. For ESN-based routing, destination routing is determined by the LNG and honored by the ESRP.

The ESRP processes transfer requests using [REDACTED] [12a].

Exhibit 30 lists the routing methods for [REDACTED] [12a].



1	[REDACTED]
2	[REDACTED]
3	[REDACTED]
4	[REDACTED]
5	[REDACTED]
6	[REDACTED]
7	[REDACTED]
8	[REDACTED]
9	[REDACTED]
10	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.2.9.2. PRF Responsibilities

Exhibit 33 delineates responsibilities between TCS and MIL/PSAP for PRF services.

Exhibit 33. PRF Responsibilities

Reference #	System/Service	Responsibility		
		TCS	MIL	PSAP
PRF-01	Provide the rule provisioning web portal to MIL and PSAP personnel	R		
PRF-02	Back up the provisioning system database on a daily basis and store in the redundant data centers (includes the Policy Routing Rules)	R		
PRF-03	Document PSAP policies at turn-up and provide as part of the as-built documentation	R		
PRF-04	Assist and review policy routing rules per PSAP as part of the QA/QC process.	I	R	
PRF-05	Notify the TCS [12] when a PSAP needs to be administratively down (and brought back online) – see PSAP Abandonment Process	I		R
PRF-06	Perform the actions necessary to stop calls from routing to a particular PSAP upon authorized notice from MIL/PSAPs.	R	I	
PRF-07	Collect the alternate routing preferences from all MIL PSAPs	R		I
PRF-08	Provision the routing rules as documented and verified by MIL	R		I
PRF-09	Provision the system based on the * code information collected.	R		I
PRF-10	Provide the names and email addresses for the users of the system	I		R
PRF-11	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R	

Legend: “R” Responsible, “I” Informed, “C” Consulted



2.2.9.3. PRF Proposal References

Exhibit 34 lists the applicable proposal and RFP references for PRF.

Exhibit 34. PRF Proposal References

Proposal Section #	Proposal Section Title
7.2.5.6	Routing Policies – [RFP 6.2.5.6]
7.2.6.2	PRF Routing – [RFP 6.2.6.2]
7.2.6.3	Legacy (PSAP) Routing – [RFP 6.2.6.3]
7.2.6.4	Rule-Sets – [RFP 6.2.6.4]
7.2.6.5	Variables – [RFP 6.2.6.5]
7.2.6.6	Configurable Subscription – [RFP 6.2.6.6]
7.2.6.8	Final Session Routing – [RFP 6.2.6.8]
7.2.6.9	Invalid Rules – [RFP 6.2.6.9]
7.2.7.1	Web Access – [RFP 6.2.7.1]
7.2.7.2	Rule-Set Changes – [RFP 6.2.7.2]
7.2.7.3	Portal Access – [RFP 6.2.7.3]
7.2.7.5	Backup – [RFP 6.2.7.5]
7.2.7.6	Example Rule-Sets – [RFP 6.2.7.6]

2.2.10. Spatial Information Function

2.2.10.1. SIF Description

The SIF is essential for the acquisition, Quality Assurance (QA)/Quality Control (QC), and staging of data for the ECRF and LVF.



[12a]



Steps that occur:

1. Customer Uploads data
2. Standardize
3. QC
4. Coalesce into statewide set
5. QC
6. Reports generated
7. Update portal Server
8. Update ECRF/LVF

SIF Tools Configuration and Remote Installation Phase

The steps for the SIF implementation are listed below.

Configuration

TCS' subcontractor, [12a] will configure the [12a] map and enterprise GIS data management solution to meet MIL's preferred system configuration and operational workflows. This information is gathered by working with MIL and participating agencies to develop a standard that meets the needs of MIL and the NG9-1-1 system. For example:

- What different GIS formats/schemas/file types will be uploaded?
- What is the statewide schema going to be?
- What QC does the state want to see vs agencies?
- What are the different roles of the participants in the system?



- How should discrepancies be handled?
- Are any layers going to come from the state or all from participating agencies (IE: boundaries)?

Address locators are a required component of the [12a] geocoding engine used in [12a] to search for features. Address locators define the process for searching [12a] will build and configure the address locators used for the solution. They allow users to find address locations throughout a variety of individual reference layers such as streets, parcels, and address points.

Remote Installation

Software installation will occur remotely prior to training. PSAPs must allow remote access to their workstations where the system will be installed. [12a] Implementation Specialists will coordinate with MIL's IT department to successfully complete remote installation.

Training

The SIF training includes:

1. Core [12a] tool functionality
2. GIS data request management
3. Downloading GIS data from the GIS Portal
4. [12a] Discrepancy Viewer functionality
5. Accessing QA/QC reports via GIS Portal or [12a] Discrepancy Viewer
6. Managing QA/QC exceptions
7. Training content and materials will be provided to assist participants to train other system users. Support materials including agendas, training formats, and scheduling will be reviewed.

Configuration of Monitoring System

[12a] will assist in configuring the [12a] Server to be monitored by TCS's monitoring solution. [12a]'s duties will include the installation of monitoring tools and [12a] configuration.

Maintenance Workflow Presentation and SIF Tools Training Phase

After project stakeholders have had time to review the preliminary documentation, the [12a] GIS Project Manager will travel on-site for a one-day working session (extendable to two days if two locations in MIL are needed). It will be followed by up to two additional conference calls and/or working web sessions to discuss and adjust the preliminary maintenance workflow diagrams. The final maintenance workflows will be distributed and discussed during an on-site meeting with stakeholders involved in GIS data editing, data management, and submission.

During this same on-site meeting, the GIS Project Manager also will provide a train-the-trainer session focusing on how to incorporate [12a]'s GIS Data Management tools into the new maintenance workflows. Training curriculum includes:

- Core [12a] Server tool functionality



- GIS data request management
- Downloading GIS data from the GIS portal
- [12a] Discrepancy Viewer functionality
- Accessing QA/QC reports via GIS portal or [12a] Discrepancy Viewer
- Managing QA/QC exceptions

Training content and materials will be provided to assist participants to train other system users. Support materials – including agendas, training formats, and scheduling – will be reviewed. Training will occur in conjunction with the workflow presentation.

[12a] will work with MIL to establish a mutually agreeable daily schedule for maintenance updates and provisioning, including a daily deadline for local authorities to submit GIS changes for processing. Data submitted before the daily deadline will undergo quality control validation checks and be sent to TCS for provisioning within 24 hours, [12a]; datasets that pass validation checks will be processed to TCS for provisioning to the ECRF; and datasets that do not pass validation checks will be returned to the local authority for resolution. Data submitted after the daily deadline will be processed after the following day's deadline.

SIF Operations Phase

The GIS dataset will be continuously updated in the [12a] Server GIS portal, which will serve as a SIF in the state's NG9-1-1 system.

This will result in a stand-alone GIS function that can provision to the ECRF and LVF to allow those functional elements to provide routing instructions for incoming calls to the correct PSAP, as well as provide the framework for developing a single, seamless, statewide GIS dataset.

[12a] will maintain "five nines" availability, as the [12a] Server is designed in such a way that no single point of failure will prevent the system from operating. To further enhance database availability, the dataset is moved to the individual systems running the functional elements of the system. In the unlikely event of a failure, alternative methods of provisioning data [12a] could be used until the system is operational again, while no critical NG9-1-1 functional elements are compromised.

Quality Assurance/Quality Control Phase

Before GIS data can be used for routing 9-1-1 calls and validating civic locations in an NG9-1-1 system, the data's accuracy and integrity must be validated through a series of data-specific, thorough QA/QC procedures. [12a]

[12a]. The QA/QC plan will be discussed during the project initiation and GIS data management collaboration meetings.

As part of the GIS maintenance workflow development process, a [12a] GIS Project Manager will collaborate with project stakeholders to develop a formal QA/QC plan. The QC approach, including regular communication of QA/QC results to local GIS entities, will be documented. The plan also will detail initial ongoing QC processes to be performed on local GIS data submitted to [12a] and into the SIF.



The final QA/QC Plan will be submitted to project stakeholders for review and approval prior to initiating any managed GIS services.

When updates are submitted by individual counties, multiple automated and manual QC processes are performed prior to coalescing the updates into the statewide GIS dataset to ensure proper topology and data integrity. Exhibit 35 lists the GIS data layers and their associated QC processes.

Exhibit 35. GIS Data Layers and Quality Control Processes

GIS Data Layer	Associated GIS Quality Control Processes
Road Centerlines	Address Range Audit – [redacted] [12a]
	Topology Audit – [redacted] [12a]
	Missing Attribute Audit – to identify missing or invalid values in pertinent attribute fields
	Road Name Audit – to ensure proper road name standardization
	Length Audit – [redacted] [12a]
Address Points	Address Spacing Audit – to identify duplicate addresses
	Address Missing Attribute Audit – to identify missing or invalid values in pertinent attribute fields
	Address Sanity Audit – to ensure logical assignment of house numbers with respect to centerline
Boundary Layers	Topology Audit – to locate gaps and overlaps in polygon coverage
	Missing Attribute Audit – to identify missing or invalid values in pertinent attribute fields
	Duplicate Audit – [redacted] [12a]
Multilayer Topology	Verifies road centerline segments are broken where they cross any ESN, community, or PSAP boundaries, ensuring that addresses (based on address ranges) are properly located within the correct community and ESN on the map. Boundaries that run parallel to road segments should be snapped to those road segments at each vertex.

GIS error reports will be generated for updates that do not pass QC. These reports will be transmitted to the sending MIL and, optionally, to stakeholders at MIL level for performance monitoring.

Handling anomalies

There will be an “exception” field in the GIS data that allows issues to pass through the QC check when they are not errors but would otherwise be flagged. E.g., if a road segment has both odd and even range values on the same side of the road, this would come up as an error in our QC check; if the county/city determined the ranges are correct, however, it could be flagged as an exception and would no longer count as an error.



Synchronization with the MSAG and ALI Database Phase

[12a] will provide MIL and local authorities with quarterly (four times per year) reports comparing each county's GIS data to its Master Street Address Guide (MSAG) and ALI database. A schedule for quarterly delivery of current MSAG and ALI database for each entity to [12a] will be discussed as part of the GIS workflow development meeting.

First, [12a] will compare the MSAG and the street centerline layer. These procedures will verify that street names are spelled consistently and ESN and community attributes are synchronized.

Second, [12a] will compare house number and street name values in the ALI database against the address point and street centerline layers. Road name inconsistencies, incorrect address ranges, and missing address points or road segments will be identified. This process also will compare ESN and community information to confirm whether ALI database addresses locate within the appropriate boundaries in the GIS map data.

These audits will provide local 9-1-1 authorities with the knowledge needed to synchronize their GIS data to the MSAG and ALI database, as well as a metric for measuring progress toward the needed synchronization level. The quality of the data included in the statewide dataset is ultimately the responsibility of individual counties.

The MSAG and ALI database must be submitted county-by-county. Statewide data records will not be accepted.

2.2.10.2. SIF Responsibilities

Exhibit 36 delineates responsibilities between TCS and MIL for SIF services.

Exhibit 36. SIF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
SIF-01	Review the map data structure and deliver a written document outlining any required modifications to the file structure or file naming <ul style="list-style-type: none"> Make recommendations on how to make those modifications to create an acceptable format for successful integration into the [12a] Server Report any ISSUES regarding preferred configurations which may affect the system performance and discuss options 	R	I
SIF-02	Coordinate and identify miscellaneous GIS map data layers which may enhance [12a] Server	R	I
SIF-03	Initially design and set up the [12a] map documents [12a] (layers, layer order, layer visibility, scale dependent display, symbology, labeling, etc.) based on MIL's preferences	R	I
SIF-04	Build and configure address locators for geocoding	R	
SIF-05	Configure and test optimized GIS SERVICES and enable capabilities (e.g., map, feature, geocode, etc.)	R	
SIF-06	Set up and configure map caching	R	
SIF-07	Publish optimized GIS SERVICES	R	I



Reference #	System/Service	Responsibility	
		TCS	MIL
SIF-08	Conduct SIF training at [12a] over a two-concurrent-day period	R	I
SIF-09	Deliver "train-the-trainer" training	R	I
SIF-10	Maintain the SIF server in "five nines" availability	R	
SIF-11	Create, configure, and load [12] address locators for simple address lookups	R	I
SIF-12	Design [12a] map documents [12] for [12a] Server (layers, layer order, layer visibility, scale dependent display, symbology, labeling, etc.) based on MIL's preferences	R	I
SIF-13	Develop, configure, test, and publish [12a] map SERVICES	R	I
SIF-14	Configure and make available the [12a] Discrepancy View licensing	R	I
SIF-15	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures	I	R
SIF-16	Provide [12a] reports comparing each county's GIS data to its MSAG and ALI database	R	I
SIF-17	Authorize TCS to acquire ALI and MSAG data from incumbent providers.	I	R

Legend: "R" Responsible, "I" Informed, "C" Consulted

2.2.10.3. SIF Proposal References

Exhibit 37 lists the applicable proposal and RFP references for SIF.

Exhibit 37. SIF Proposal References

Proposal Section #	Proposal Section Title
7.2.8.6.4	GIS Database Validation – [RFP 6.2.8.6.4]
7.2.8.6.5	Location Errors – [RFP 6.2.8.6.5]
7.2.11.4	Minimum Initial Base Data – [RFP 6.2.11.4]
7.2.11.7	Database Maintenance – [RFP 6.2.11.7]
7.2.12	Spatial Information Function (SIF) – [RFP 6.2.12]
7.2.12.1	SIF Interfaces – [RFP 6.2.12.1]
7.2.12.2	24x7x365 Availability – [RFP 6.2.12.2]
7.2.12.3	Processing Time – [RFP 6.2.12.3]
7.2.12.4	Quality Assurance/Quality Control (QA/QC) – [RFP 6.2.12.4]
7.2.12.6	Performance Measurements – [RFP 6.2.12.6]
7.2.11.8	ALI/MSAG Synchronization – [RFP 6.2.11.8]

2.2.11. Emergency Call Routing Function (ECRF)

2.2.11.1. ECRF Description

The [12a] ECRF conforms to NENA i3 standards, and operates as a web server within the NGCS to service Location to Service Translation (LoST) queries from the ESRP, CPE, and



other approved ESInet elements. [12a]

The ECRF accepts the following elements from the SIF:

- Street/road centerline
- PSAP boundary
- County boundary
- Emergency Service Zone (ESZ) with associated ESN

The ECRF processes FindService requests based on the following inputs:

- MSAG valid civic address
- Point data
- Circles
- Arc bands
- Polygons

The ECRF supports the following LoST [12a] protocol messages:

- [12a]

Loading Process:

- [12a]
- QA check run on all data loaded into the staging database, reporting:
 - Gaps/overlaps
 - Conflicts
- Product ECRF GIS databases updated through data replication

The initial NG9-1-1 stand-alone GIS dataset for routing calls is based on existing data available within MIL and from county 9-1-1 authorities. This includes mechanisms for continuously updating the dataset to produce seamless, statewide coverage.

The solution includes a variety of core components for acquiring location GIS data updates, performing GIS data transformation and GIS data normalization, executing automated QA/QC checks, reporting discrepancies back to counties, and providing a seamless statewide GIS dataset.

Routing changes can be performed through data management processes by TCS personnel

[12a]

TCS will provide the county 9-1-1 authority with exports of the production GIS database if needed.



2.2.11.2. ECRF Responsibilities

Exhibit 38 delineates responsibilities between TCS and MIL for ECRF services.

Exhibit 38. ECRF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
ECRF-01	Operational status	R	
ECRF-02	Data management	R	
ECRF-03	ECRF interfaces available	R	
ECRF-04	Update the ECRF weekly	R	
ECRF-05	Network connection from ESRP to ECRF	R	
ECRF-06	ESRP readiness to send/receive [12a]	R	
ECRF-07	Replicate the master GIS database from the SIF and maintain interconnection with the ECRF databases	R	
ECRF-08	Correct GIS data inconsistencies, errors, or anomalies for data reconciliation	R	
ECRF-09	Research problems related to the GIS data layers, as necessary, and applying any required configuration changes	R	
ECRF-10	Provide QA and “publish” any routing data received from the SIF/single master GIS database before automatically updating production routing databases	R	
ECRF-11	Monitor database availability and health, replication topology, and maintenance plans, and provide upkeep of database maintenance plans, database schema, and replication topology	R	
ECRF-12	Manage all configuration questions and changes, including, without limitation, production spatial routing changes and GIS database updates	R	
ECRF-13	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.2.11.3. ECRF Proposal References

Exhibit 39 lists the applicable proposal and RFP references for ECRF.

Exhibit 39. ECRF Proposal References

Proposal Section #	Proposal Section Title
7.2.8	ECRF [RFP 6.2.8]
7.2.8.3	ECRF Interface – [RFP 6.2.8.3]
7.2.8.4	ECRF Access – [RFP 6.2.8.4]
7.2.8.6.2	GIS Updates – [RFP 6.2.8.6.2]
7.2.8.6.3	Shape Files – [RFP 6.2.8.6.3]
7.2.8.6.6	Routing – [RFP 6.2.8.6.6]
7.2.11.2	ECRF and LVF Access – [RFP 6.2.11.2]



2.2.12. Location Validation Function

2.2.12.1. LVF Description

[12a]

[12a] Spatial Router LVF Implementation Phase

[12a] will implement [12a] Spatial Router LVF in TCS' data center.

[12a] Spatial Router LVF Software Training

The [12a] Spatial Router Training Plan is outlined in the table below. Training will be provided on-site by a [12a] implementation professional.

Exhibit 40 [12a] Spatial Router LVF Training

Course Title	Maximum Total Training Hours	Delivery Method	Number of Sessions
[12a] Spatial Router LVF Training	[12a] s	Web Based – Can be recorded by MIL for rebroadcast.	1

[12a] Spatial Router training will focus primarily on the functions and architecture of the software. The MIL will be responsible for determining the appropriate staff to participate in the training sessions. Exhibit 41 lists the [12a] Spatial Router training topics.

Exhibit 41. LVF Training Topics

LVF Training Topics		
[12a] Spatial Router Workspace	Servers Pane	All Performance Pane
Viewing Reports	Viewing Logs	Provisioning Stages
Troubleshooting Scenarios	Logging In	Logging Off
Details Pane	Reports Toolbar	Provisioning Overview
Quality Control	Managing System Access	Queries Pane
Discrepancy Report	Error Logging	

2.2.12.2. LVF Responsibilities

Exhibit 42 delineates responsibilities between TCS and MIL for LVF services.

Exhibit 42. LVF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LVF-01	Implement the LVF on the network TCS provides to MIL and make accessible to MIL PSAPs and CSPs	R	
LVF-02	Data management	R	
LVF-03	Deliver [12a] spatial router training	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
LVF-04	Provide the list and of individuals authorized to use the LVF		R
LVF-05	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.2.12.3. LVF Proposal References

Exhibit 43 lists the applicable proposal and RFP references for LVF.

Exhibit 43. LVF Proposal References

Proposal Section #	Proposal Section Title
7.2.9	Location Validation Function (LVF) – [RFP 6.2.9]
7.2.11.2	ECRF and LVF Access – [RFP 6.2.11.2]

2.2.13. Media Server

2.2.13.1. Media Server Description

The media server is the NGCS that handles conference setup and teardown [12a] [REDACTED]. The service currently handles no-hold and consultation hold-type transfers. Exhibit 44 lists media server methods and supported PSAP CPE.

Exhibit 44. Media Server Methods and PSAP CPE Supported

Method	PSAP CPE Supported
SIP REFER	i3 compliant PSAP CPE
DTMF in IP	IP connected PSAP CPE
*code translation	LPG connected PSAPs
#code translation	LPG connected PSAPs

2.2.13.2. Media Server Responsibilities

Exhibit 45 delineates responsibilities between TCS and MIL for media server services.

Exhibit 45. Media Server Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
MEDIA-01	Media servers available to the ESnet	R	
MEDIA-02	Complete provisioning to support the chosen transfer method for each PSAP		
MEDIA-03	Document the PSAP’s chosen transfer method at turn-up and provide as part of the as-built documentation	R	
MEDIA-04	Assist in the collection and review of transfer methods per PSAP	I	R



Reference #	System/Service	Responsibility	
		TCS	MIL
MEDIA-05	Collect the transfer method preferences from all MIL PSAPs	R	I
MEDIA-06	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

2.2.14. Border Control Function

2.2.14.1. BCF Description

The BCF is the NGCS that provides [12a]. The [12a] functionality mediates all calls ingressing from the LNG/LSRG as well as any direct SIP ingress from VoIP or other CSPs, and it provides protection from [12a] attacks. [12a]

Exhibit 46. BCF Codec Table

Codec	
[12a]	[12a]
[12a]	[12a]
[12a]	[12a]
[12a]	[12a]
[12a]	[12a]
[12a]	[12a]
[12a]	[12a]
[12a]	[12a]



2.2.14.2. BCF Responsibilities

Exhibit 47 delineates responsibilities between TCS and MIL for BCF services.

Exhibit 47. BCF Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
BCF-01	Implement ingress BCF functionality at each of the data centers	R	
BCF-02	Implement egress BCF functionality at each of the data centers	R	
BCF-03	Implement firewall functionality at each of the PSAPs	R	
BCF-04	Collect and provide information from each PSAP regarding non-TCS-provided ESnet connected SERVICES each PSAP needs to access	I	R
BCF-05	Review each firewall-related access request from MIL	R	I
BCF-06	Implement each approved firewall-related access request from MIL	R	I
BCF-07	Accurate and timely trouble reporting and description of problems to TCS 112a , for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.2.14.3. BCF Proposal References

Exhibit 48 lists the applicable proposal and RFP references for BCF.

Exhibit 48. BCF Proposal References

Proposal Section #	Proposal Section Title
7.2.4	BCF – [RFP 6.2.4]
7.2.4.2	SIP – [RFP 6.2.4.2]
7.2.4.3	Audio CODEC Selection – [RFP 6.2.4.3]
7.2.4.4	Silence Suppression – [RFP 6.2.4.4]
7.2.4.5	Comfort Noise – [RFP 6.2.4.5]

2.2.15. Network LIS

2.2.15.1. NLIS Description

The NLIS encompasses the evolution of LOCATION DATA from the existing legacy ALI to TCS’ ALI, to a Location Database (LDB) and support of LIS as CSPs implement them.

Phase 1: Use of the Existing ALI Database

PSAPs cutover to the TCS ESInet will connect the CPE to serial/IP converters, and the new MPLS network will transport NENA 04-001 requests for ALI to the existing ALI database.



Phase 2: Cutover PSAPs over to [12a] ALI

PSAPs cutover to the TCS ESInet will connect the CPE to serial/IP converters, and the new MPLS network will transport NENA 04-001 requests for ALI to the new [12a] ALI database.

Phase 3: Full Location Database Implementation

During the implementation phase for the Location Database (LDB) TCS will provide the capability for i3 PSAPs to request ALI via [12a].

TCS' ALI service, [12a] ALI, provides the necessary functionality for MIL and PSAPs to move ALI data within their control while still having the data professionally managed by TCS' ALI Quality Process and Services (AQPS) staff.

The AQPS team uses the [12a] ALI DBMS to manage MSAG and ALI information with the cooperation of MIL and CSPs. Both CSPs and PSAPs can query the ALI database via a [12a] graphical user interface (GUI).

[12a] ALI includes a [12a] tool with searching capabilities that allow "wildcard" searches and U.S. Postal Service equivalents. Exhibit 49 lists the tool's database management system (DBMS) capabilities.

Exhibit 49. DBMS Capabilities

DBMS Capabilities	
1	Search the ALI database for a telephone number record.
2	On-demand downloads of ALI or MSAG data.
3	PSAPs and CSPs can search for ALI or MSAG data records.
4	ALI Discrepancy management and MSAG change management via [12a] workflow processes.
5	Search for ALI data that matches NPA/NXX.
6	Search the MSAG database for MSAG data records that match a street address.

All interaction between the PSAP jurisdictional authority, a Competitive Local Exchange Carrier (CLEC), or another authorized user and the database management subsystem is supported through a combination of [12a] and/or secure internet- [12a] interfaces.

No Record Found (NRF) reports are made available to the service provider in accordance with NENA standards. ALI database record updates generate error and status reports that can be made available to MIL, as required.

TCS uses both on-board and off-board reporting engines to collect, compile, and report on data from [12a] ALI. The solution is set up to collect data from [12a] files to provide reports and extracts of ALI and MSAG data. The TCS [12a] monitors the health of TCS' [12a] ALI and the key processes running on the system.



ALI Quality Processes and Service

The data is managed by the TCS data integrity unit, called the AQPS. The AQPS unit is made up of data analysts who work with CSPs, 9-1-1 authorities, and other 9-1-1 stakeholders who need to access services, processes, or data via the ALI DBMS.

Key AQPS Unit Responsibilities

The AQPS team will manage to the following service intervals on key ALI change management processes. Service Intervals listed are [12a] MIL should note that initial MSAG and ALI telephone number load, as well as other initial key ALI data loads required to set up the ALI DBMS (e.g., NPA/NXX, ESN/Emergency Service agency [ESA]/English Language Translation [ELT], etc.) will take longer than the agreed to change management service intervals listed below. TCS will work with MIL to establish the data migration plan, which will involve cooperation from the existing ALI service providers. Exhibit 50 lists the Service Level Agreement (SLA) for NLIS.

Exhibit 50. Data Management Commitments for NLIS

#	Data Management Commitments for NLIS	Days
1	Management of NRF and other time-of-call ALI discrepancies. TCS will distribute NRFs to carriers/CSPs within [12a] y of them being reported by a PSAP and escalated to the AQPS team and/or retrieving NRF reports from the system.	1
2	Expired unlocked data records that have not been migrated will be deleted after 1 days of being unlocked.	1
3	MSAG record change management – up to 1 changes per day for MIL after deployment is completed.	1
4	The following have a 1 business day change management process cycle, due to QC audit and/or verification processes:	
4.1	• NPA/NXX changes (must be verified via [12a] process)	1
4.2	• VoIP and wireless ALI steering requests	1
4.3	• ESN/ESA/ELT	1
4.4	ALI Format Changes for PSAP	1

¹ALI Format Changes can take at least 1 days and in some cases longer. The PSAP must coordinate with their CPE provider before changes can be made and tested

²MIL/PSAPs will work with TCS' AQPS team in advance to plan large redistricting/addressing changes so large scale changes can be completed efficiently.

ALI Record Error Resolution

TCS' AQPS team uses procedures based upon those recommended in NENA 02-011. The team takes advantage of the various tools TCS has developed to resolve errors.

Automated Service Order Input (SOI) files can be processed into the [12a] ALI via [12a] for CSPs that need to process large volumes of customer telephone number record updates. Assuming all security measures are passed, the file is processed or the user is validated and file



results, including error reports, are available under the CSP's [12a]. CSPs are also able to use the [12a] SOI interface to manage smaller telephone number updates in the ALI database.

CSP Database Reconciliation

CSPs can pull full extracts of their customers' ALI data records and audit their data records against their current billing customer base. CSPs can perform customer data record corrections via an automated SOI process in which a large number of record updates can be contained in a single update file, or as a single record update via the [12a] GUI. TCS works with the CSPs to ensure they complete audits of their customer data records on a regularly scheduled basis.

2.2.15.2. NLIS Responsibilities

Exhibit 51 delineates responsibilities between TCS, MIL, and CSPs for NLIS services.

Exhibit 51. NLIS Responsibilities

Reference #	System/Service	Responsibility		
		TCS	MIL	CSPs
NLIS-01	Notification of transition to PSAPs/ECDs and CSPs	I	R	
NLIS-02	Obtaining incumbent ALI/MSAG data for transition	C	R	
NLIS-03	PSAP ALI deployment testing	R	C	
NLIS-04	MPLS network connectivity from the PSAP to the ALI database	R		
NLIS-05	9-1-1 database management	R	C	
NLIS-06	Training for STATE and CSP personnel	R	C	
NLIS-07	Use NENA 2.1 file format and NENA 04-001 provisioning interfaces	I	I	R
NLIS-08	Load data into the TCS [12a] ALI DBMS based on TCS published PROJECT PLAN for ALI transition	I	I	R
NLIS-09	Service order process oversight	R		
NLIS-10	MSAG build and maintenance	R		
NLIS-11	ESN/ESA/ELT build and maintenance	R		
NLIS-12	Company ID (COID) build and maintenance	R		
NLIS-13	NPA/NXX build and maintenance	R		
NLIS-14	MSAG community name build and maintenance	R		
NLIS-15	Out of sync data error correction and referral	R		
NLIS-16	ALI discrepancy management and reporting	R		
NLIS-17	Telephone number data extracts and distribution	R		
NLIS-18	MSAG data extracts and distribution Location number portability oversight respective to the ALI DBMS lock and unlock processes	R		
NLIS-19	Metrics and reporting	R		
NLIS-20	Data retention is [12a]	R		
NLIS-21	Transaction history will be stored on the ALI DBMS for a period up to 11 days	R		



Reference #	System/Service	Responsibility		
		TCS	MIL	CSPs
NLIS-22	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R	

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.2.15.3. NLIS Proposal References

Exhibit 52 lists the applicable proposal and RFP references for NLIS.

Exhibit 52. NLIS Proposal References

Proposal Section #	Proposal Section Title
11.2.2	Network Location Information Service (NLIS) – [RFP 6.2.2]
7.2.2.2	NLIS Support for Legacy ALI – [RFP 6.2.2.2]

2.3. Other Provided Services

2.3.1. Logging

2.3.1.1. Logging Description

Architecture

Transactional logs from the NGCS functional elements, LSRG, LNG, BCF, ESRP, PRF, ECRF, LVF, LPG, and ALI are created using the NENA i3 logging methodology. The events will be captured in Universal Coordinated Time (UTC) and displayed in Pacific Time Zone (PTZ) through the portal.

These logs will display, at a minimum, a process instance identifier and the date and time-stamped record (PTZ) of each SIP, LoST, or ALI message processed.

In the transactional log database, the most commonly used SIP headers (To:, from:, Contact:, etc.) and the request URI will be parsed into dedicated fields in the transactional log database.

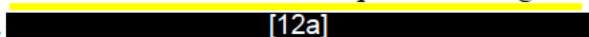
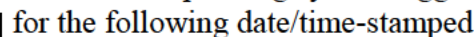
Functional Element Logging



Operational Message Logging



Operational Log Definition

At a minimum, all elements, processes, or services will process and date/time-stamp operational log entries into the dedicated local raw operational log files and into an operating system logging facility (e.g.,  [12a]  for the following date/time-stamped events:



- Every time the process is started and any relevant details of how it was started (e.g., command line, monitor program, startup parameters, etc.).
- Any major change in the process state, such as process going from online to standby, shutting down, etc. If possible, a change of process state should be accompanied by a reason (e.g., “operator commanded shutdown” or “memory overflow”).
- Significant nonroutine events, including [12a]
 [REDACTED]
 [REDACTED]
- If the process supports operator logins, the operational log will show every login attempt, user and time, successful or unsuccessful, the operator commands issued, and logout time.

2.3.1.2. Logging Responsibilities

Exhibit 53 delineates responsibilities between TCS and MIL for logging services.

Exhibit 53. Logging Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LOG-01	Maintain local raw transactional logs for at least 30 days.	R	
LOG-02	Consolidate raw transactional log files and maintain offline for [12a].	R	
LOG-03	Display all logged events in PTZ time.	R	
LOG-04	Provide a portal to transactional log events that is [REDACTED] [12a]	R	
LOG-05	Provide read-only access to the transactional log database information.	R	
LOG-06	Support the creation of new reports based on user-specified selection of the transactional log events.	R	
LOG-07	Support print and download capabilities from the transactional log portal.	R	
LOG-08	Maintain local raw operational logs for at least 30 days.	R	
LOG-09	Consolidate raw operational log files and maintain for [12a].	R	
LOG-10	Display all logged events in PTZ time.	R	
LOG-11	Provide a portal to operational log events that is [REDACTED] [12a]	R	
LOG-12	Provide read-only access to the operational log database information.	R	
LOG-13	Support the creation of new reports based on user-specified selection of the operational log events.	R	
LOG-14	Support print and download capabilities from the operational log portal.	R	
LOG-15	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted



2.3.1.3. Logging Proposal References

Exhibit 54 lists the applicable proposal and RFP references for logging.

Exhibit 54. Logging Proposal References

Proposal Section #	Proposal Section Title
7.2.3.4	LNG Call Recording – [RFP 6.2.3.4]
7.2.4.9	BCF Session Recording – [RFP 6.2.4.9]
7.2.5.11	ESRP Session Recording – [RFP 6.2.5.11]
7.2.7.4	Logging – [RFP 6.2.7.4]
7.2.8.5	ECRF Logging – [RFP 6.2.8.5]
7.2.21.1	General – [RFP 6.2.21.1]
7.2.21.2	ESInet Element Logs – [RFP 6.2.21.2]
7.2.21.3	ESInet Element Log Consolidation – [RFP 6.2.21.3]
7.2.21.4	Log File Redundancy – [RFP 6.2.21.4]
7.2.21.5	Consolidated Log File Retention – [RFP 6.2.21.5]
7.2.21.6	Consolidated Raw Transactional Logs: Database – [RFP 6.2.21.6]
7.2.21.7	Database Search – [RFP 6.2.21.7]
7.2.21.8	Database Tools – [RFP 6.2.21.8]
7.2.21.10	Operational Log Events – [RFP 6.2.21.10]
7.2.21.11	Operational Log Tools – [RFP 6.2.21.11]

2.3.2. Reporting

2.3.2.1. Reporting Description

The solution will provide the reports with the content described in the applicable proposal and RFP references and in the required format and by the delivery method.

Failed calls report format: **[12a]**

- County of call origination
- PSAP for call destination (if determinable)
- ANI/pANI
- Callback number (CBN) – wireless/VoIP (optional)
- Carrier (from which the call originated)
- Start time of call MM/DD/YYYY, hh.mm.ss.s PTZ
- End time of call MM/DD/YYYY, hh.mm.ss.s PTZ

The report can be sorted based on:

- County
- PSAP (where determinable)



- Carrier

BCF log file format: [12a]

- Date and time of session: MM/DD/YYYY hh.mm.ss.s PTZ
 - Start
 - End
- ANI of session
- Calling Party Number (CPN) of session (if available and different from ANI)
- Session type (e.g., wireline, wireless, VoIP)
- Carrier for call (optional)
- Media (e.g., audio, text, video)
- Mean Opinion Score (MOS) (originating and terminating)
- Status (e.g., successful, busy, reorder, ring no answer)

ESRP log file format: [12a]

- Date and time of call: MM/DD/YYYY hh.mm.ss.s PTZ
 - Start
 - End
- ANI of call
- CPN of call (if different from ANI)
- Carrier for call
- Media (e.g., audio, text, video)
- Status (e.g., successful, busy, reorder, ring no answer)

LNG log file format: [12a]

- Date and time of call: MM/DD/YYYY hh.mm.ss.s PTZ
 - Start
 - End
- ANI of call
- CPN of call (if different from ANI)
- Carrier for call
- Call type (i.e., wireline, wireless, VoIP)
- MOS
- Status (e.g., successful, busy, reorder, ring no answer)



2.3.2.2. Reporting Responsibilities

Exhibit 55 delineates responsibilities between TCS and MIL for reporting services.

Exhibit 55. Reporting Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
REP-01	[12a]	R	
REP-02	LNG log files shall be extracted on a [12a] basis and sent via [12a]	R	I
REP-03	Review LNG log files on a [12a] basis and present a single document of questions within [1] business days of receipt of the LNG log files.	I	R
REP-04	BCF log files shall be extracted on a [12a] basis and sent via [12a]	R	I
REP-05	Review BCF log files on a [12a] basis and present a single document of questions within [1] business days of receipt of the BCF log files.	I	R
REP-06	ESRP sessions log files shall be extracted on a [12a] basis and sent via [12a]	R	I
REP-07	Review ESRP log files on a [12a] basis and present a single document of questions within [1] business days of receipt of the ESRP log files.	I	R
REP-08	Provide portal access via [12a]	R	
REP-09	Provide a method (phone request or portal) for MIL to request and receive within [12a] a BCF, ESRP, or LNG extract in accordance with the formats listed above, and within the requested date/time range.	R	I
REP-10	Review manually requested log files and present a single document of questions within [1] business days of receipt of the log files.	I	R
REP-11	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures	I	R
REP-12	Provide access via a portal to transactions, including related ALI database transactions, related to a single call identified by time (PTZ), calling number, source, ultimate destination, or SIP Call-ID header.	R	I
REP-13	Provide access via a portal to a set of calls based on source, ultimate destination, calling number, and conditioned by a specified interval.	R	I
REP-14	Provide access via a portal to call volume reports (counts) based on source destination or call handling (e.g., success, failure [reason], transferred, etc.).	R	I

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.3.2.3. Reporting Proposal References

Exhibit 56 lists the applicable proposal and RFP references for reporting.

Exhibit 56. Reporting Proposal References

Proposal Section #	Proposal Section Title
11.1.16	Failed Calls Report – [RFP 6.1.16]



Proposal Section #	Proposal Section Title
7.2.3.5	LNG Call Reporting – [RFP 6.2.3.5]
7.2.4.10	BCF Session Reporting – [RFP 6.2.4.10]
7.2.5.12	ESRP Session Reporting – [RFP 6.2.5.12]
7.2.21.9	Database Access – [RFP 6.2.21.9]

2.3.3. Statewide GIS Database

2.3.3.1. Statewide GIS Database Description

TCS will use [12a]'s services to create an initial statewide GIS dataset for NG9-1-1 by combining GIS data layers from STATE and local entities, including all of the county 9-1-1 authorities. The preferred method of local data submission from individual counties or regional authorities is via upload to the [12a] Server GIS portal or [12a]. Entities unable to upload data via this method will have the option to use [12a] replication to submit data. [12] geodatabase replication would be configured during the initial load stage for source entities capable of using [12a].

GIS Services: Creation of Statewide Geodatabase Phase

This initial GIS dataset will be statewide, in that it will incorporate existing data throughout the state. In order to route calls to the correct dispatch center using this GIS data in the proposed ECRF, and subsequently forward them to the appropriate responder, the following minimum GIS layers will be required throughout the state:

- Street/road centerline, with road ranges
- PSAP boundary
- County boundary
- ESZ boundaries

If the street/road centerline and county boundary layers are not available from the state, individual counties, or regional authorities, [12a] can populate them based upon publically available sources such as the [12a]. If PSAP and/or ESZ boundaries are not available, [12a] can develop or synchronize the road centerline layer to the MSAG for individual counties at an additional cost and under a separate contract between the individual county/region and [12a].

In order to create topological accuracy across county boundaries, [12a] also will create reference layers along county boundaries to which local authorities can match road centerlines and boundary polygons.

Additional layers (included as an optional, additional price) also can be integrated into the GIS dataset, but are not required to form an initial base dataset capable of routing incoming 9-1-1 calls. The optional layers include:

- Site/structure addresses, including subparcel data as it becomes available
- State boundaries



- Municipal boundaries
- Unincorporated community boundaries
- Neighborhood boundaries (e.g., subdivisions, gated communities)

While [12a] will provide ongoing QA/QC audits and the data updates that fail QC checks will not be provisioned into the ECRF, the quality of the data included in the statewide dataset is ultimately the responsibility of individual counties.

Once received, source GIS data will be run through rigorous QC checks to ensure it meets the STATE of Washington's NG9-1-1 criteria. Any problems detected will be referred back to source 9-1-1 entities for resolution.

To facilitate the creation of a uniform, statewide GIS base map, automated schema and geodetic transformation procedures will be executed to assimilate the source GIS data layers into an authoritative GIS data model that is compliant with NENA's emerging and evolving NG9-1-1 data standards. The individual GIS data layers will then be merged into a statewide dataset.

The proposed system accommodates differing data models and geodetic systems from disparate 9-1-1 GIS data sources. Counties will be able to continue working with their existing data structure, if needed, and still have updates incorporated into the statewide dataset.

Note: Local 9-1-1 authorities will have secure, administrative, read-only access and export capabilities to the data records within the GIS database. [12a] will provide local 9-1-1 authorities with exports of the GIS database. No direct access to the GIS data within the ESInet will be given to a county 9-1-1 authority.

[12a] will not retain any rights of ownership, copyrights, or distribution rights for the data created or coalesced for the STATE of Washington. All data will be for use by MIL at its discretion. In addition, [12a] has an established level of security and follows standard operating procedures that eliminate the potential of unauthorized access to confidential customer data.

Maintenance Workflow Development Phase

After GIS data is initially incorporated into the statewide geodatabase, authoritative agencies may continuously update the data to ensure the data used for 9-1-1 services is the most current. In order to establish a workflow that will allow for regular updates, [12a] will host an on-site extract/transform/load (ETL) and GIS data management collaboration meeting during the same on-site trip as the project initiation meeting.

[12a]'s Project Manager will work with project stakeholders to identify GIS data sources for the system as well as key roles in the GIS data workflow process. In addition, the following will be discussed:

- Existing GIS workflows within the STATE of Washington
- GIS data quality expectations and data remediation requirements
- Local data source field mapping to statewide accepted data schema



- Developing mechanisms to work toward a true seamless, gapless statewide dataset through guidelines and standard operating procedures for local jurisdictions maintaining the source GIS data
- Workflows that will allow for changes without fatal QC errors to be consistently processed within [12] hours of a mutually agreeable daily submission deadline, [12a]

[12a] will conduct an initial GIS workflow analysis. Local GIS data sources as well as specific roles and responsibilities in the GIS data exchange process will be documented. Existing workflows will be reviewed and modifications will be identified to incorporate the software and services included with the solution.

The data schema will need to be finalized during the ETL and GIS data management collaboration meeting, as it will provide the base for the ETL processes to be developed by [12a]

After the review, [12a] will develop and provide a preliminary copy of the enhanced and new maintenance workflow diagrams. The recommended NG9-1-1 GIS workflows will cover roles, responsibilities, and activities, including:

- Local authoritative GIS data update incorporation, including reviewing, tracking, and management by source 9-1-1 entities
- Review, editing, and management of addressing information from other authoritative sources by source 9-1-1 entities
- Provisioning GIS updates into the regional or statewide GIS dataset
- Workflow for handling QA/QC error reports and subsequent re-provisioning
- Identifying mechanisms for propagating GIS changes to the ECRF and LVF servers

2.3.3.2. Statewide GIS Database Responsibilities

Exhibit 57 delineates responsibilities between TCS, MIL, and PSAPs for statewide GIS database services.

Exhibit 57. Statewide GIS Database Responsibilities

Reference #	System/Service	Responsibility		
		TCS	MIL	PSAPs
GISDB-01	Operation	R		
GISDB-02	Data management	R		
GISDB-03	Backup/restore	R		
GISDB-04	Network access to MIL	R		
GISDB-05	Layers provided: <ul style="list-style-type: none"> • Street/road centerline • PSAP boundary • County boundary 	R		



Reference #	System/Service	Responsibility		
		TCS	MIL	PSAPs
	<ul style="list-style-type: none"> ESZ (with associated ESN) 			
GISDB-06	Managed SERVICES <ul style="list-style-type: none"> Acquire local GIS data updates Data transformations and normalization Automated QA/QC (up to daily) Report GIS discrepancies 	R		
GISDB-07	Quarterly GIS/MSAG/ALI comparison reports	R		
GISDB-08	Submission of MSAG/ALI data by county			R
GISDB-09	Quality of the GIS data	I		R
GISDB-10	Accurate and timely trouble reporting and description of problems to TCS [REDACTED] [12a] [REDACTED], for events where TCS has no visibility, per established reporting procedures		R	R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.3.3.3. Statewide GIS Database Proposal References

Exhibit 58 lists the applicable proposal and RFP references for the statewide GIS database.

Exhibit 58. Statewide GIS Database Proposal References

Proposal Section #	Proposal Section Title
7.2.8.6	GIS Routing Database (Function) – [RFP 6.2.8.6]
7.2.8.6.1	GIS Compliance – [RFP 6.2.8.6.1]
7.2.8.6.7	GIS Database Access – [RFP 6.2.8.6.7]
7.2.11	Statewide GIS Database – [RFP 6.2.11]
7.2.11.1	GIS Database Availability – [RFP 6.2.11.1]
7.2.11.5	Hardware and Software – [RFP 6.2.11.5]
7.2.11.6	Database Maintenance – [RFP 6.2.11.6]
7.2.11.9	GIS Data Ownership – [RFP 6.2.11.9]
7.2.12.5	Data Conversion/Normalization – [RFP 6.2.12.5]

2.3.4. Data Provisioning

2.3.4.1. Data Provisioning Description

TCS manages the data necessary for the operation of the system. Change requests from MIL personnel will be processed by TCS staff.

2.3.4.2. Data Provisioning Responsibilities

Exhibit 59 delineates responsibilities between TCS and MIL/PSAPs for data provisioning services.



Exhibit 59. Data Provisioning Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
DATAPR-01	Process, input, quality check, and activate changes to the data necessary to operate the system within [11] business days, or returned to the originator with notification of exceptions that must be resolved before the updates can be processed.	R	I
DATAPR-02	Authorize TCS to obtain the data and information necessary to configure the system.		R
DATAPR-03	For the system data necessary to provision the system (DATAPR-01 – collected by DATAPR-02) TCS requires that MIL/PSAPs return corrected data within [11] business days after exceptions are communicated to MIL/PSAPs.	I	R
DATAPR-04	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.3.5. Multimedia

2.3.5.1. Multimedia Description

The solution uses SIP/MSRP to support text messaging from TCS Text Control Centers (TCCs). Connectivity to each of the TCCs is over MSRP.

The solution **[12a]** **[REDACTED]** delivery to PSAPs using a SIP/MSRP-enabled interface and does not support interfaces that are **[12a]** **[REDACTED]** based. Routing of text is done by location (using the ECRF) and uses policy routing rules that are unique to text vs. voice.

The solution supports pass-through routing of H.264/MPEG-4 streaming video.

2.3.5.2. Multimedia Responsibilities

Exhibit 60 delineates responsibilities between TCS and MIL for multimedia services.

Exhibit 60. Multimedia Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
MULTI-01	Request service from Washington wireless carriers	I	R
MULTI-02	Procure connectivity to TCCs	R	
MULTI-03	Implement connectivity to TCCs	R	
MULTI-04	Monitor TCC to ESInet connection	R	
MULTI-05	Procure additional equipment, connectivity, and SERVICES necessary to support streaming video ingress to the ESInet to be reimbursed by MIL.	R	I
MULTI-06	Implement associated software as necessary to support streaming video ingress to the ESInet	R	I
MULTI-07	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED] , for events where TCS has no visibility, per established reporting procedures		R



Legend: “R” Responsible, “I” Informed, “C” Consulted

2.3.5.3. Multimedia Proposal References

Exhibit 61 lists the applicable proposal and RFP references for multimedia.

Exhibit 61. Multimedia Proposal References

Proposal Section #	Proposal Section Title
7.2.4.6	Text Support – [RFP 6.2.4.6]
7.2.4.7	Text Control Center (TCC) Integration – [RFP 6.2.4.7]
7.2.4.8	Video CODEC Support – [RFP 6.2.4.8]

2.3.6. Documentation

2.3.6.1. Documentation Description

This section describes the documentation delivered with this solution per the applicable proposal and RFP requirements.

NLIS documentation includes:

- PSAP data management
- Carrier data management/SOI guide
- Basic operation overview
- Data management processes and procedures
 - Initial creation of dataset(s)
 - Maintenance of dataset(s)

PRF documentation includes:

- PRF Provisioning Guide

ECRF documentation includes:

- OTF Routing Request Guide

LVF documentation includes:

- Location Query Guide

As-built documentation includes:

- Generalized system architecture
- Call flow diagrams

PSAP documentation includes:

- Standard Operating Procedures
 - Includes Abandonment procedures



- Communication with the NOC

2.3.6.2. Documentation Responsibilities

Exhibit 62 delineates responsibilities between TCS and MIL for documentation services.

Exhibit 62. Documentation Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
DOC-01	Provide electronic copies of the PRF provisioning guide [12a] before the first PSAP is deployed	R	
DOC-02	Provide electronic copies of the NLIS [12a] ALI) documentation [12a] before [12a] ALI is implemented	R	
DOC-03	Provide the as-built documentation and updates [12a] after each PSAPs is deployed	R	
DOC-04	Provide electronic copies of the LVF – Location Query Request Guide, [12a] before the LVF is implemented	R	
DOC-05	Provide electronic copies of the NOC Standard Operating Procedures	R	

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.3.6.3. Documentation Proposal References

Exhibit 63 lists the applicable proposal and RFP references for documentation.

Exhibit 63. Documentation Proposal References

Proposal Section #	Proposal Section Title
7.2.2.3	NLIS Documentation – [RFP 6.2.2.3]
7.2.6.12	Documentation – [RFP 6.2.6.12]
7.2.8.8	ECRF Documentation – [RFP 6.2.8.8]

2.4. Operational Considerations

2.4.1. General Operations

2.4.1.1. General Operations Description

The TCS solution is a NENA i3-compliant platform committed to the “five nines” standard (99.999 percent reliability) for providing the delivery and receipt of 9-1-1 calls. The solution minimizes single points of failure; it is composed of redundant central system components that provide load sharing and load balancing with failover capability.

The solution is designed as a fully redundant system that employs automatic failover to minimize call failures. Manual intervention is not required. The solution is engineered to ensure no detrimental effects result from time changes.

2.4.1.2. General Operations Responsibilities

Exhibit 64 delineates responsibilities between TCS and MIL for general operations.



Exhibit 64. General Operations Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
GENOPS-01	All facets of the ESInet system shall be monitored on a staffed (i.e., humans always present and on duty at the monitoring location) 365 X 24	R	
GENOPS-02	The monitoring system shall maintain logs of all ESInet alarms and notifications regardless of severity level	R	
GENOPS-03	The monitoring system logs shall record any loss of capability to monitor the ESInet, either in whole or in part, and reflect the time the capability was lost or impaired and the time at which the capability was fully restored	R	
GENOPS-04	Provide root-cause analysis (RCA) for Service Impairment Level (SIL) 1 and SIL 2 events (high impact to service)	R	
GENOPS-05	Review and comment on RCA		R
GENOPS-06	Provide 24x7 monitoring and operations support	R	
GENOPS-07	Use georedundant advanced network monitoring and reporting tools (e.g., [1] [redacted]) 2a	R	
GENOPS-08	Accurate and timely trouble reporting and description of problems to TCS [12a] [redacted], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.4.1.3. General Operations Proposal References

Exhibit 65 lists the applicable proposal and RFP references for general operations.

Exhibit 65. General Operations Proposal References

Proposal Section #	Proposal Section Title
11.1.10	Time Changes – [RFP 6.1.10]

2.4.2. Availability

2.4.2.1. Availability Description

[redacted] [12a]

Site redundancy – TCS data centers with secure, monitored access in [redacted] [12a] will provide the system applications and network monitoring service. Each data center is equipped with the same software and hardware, and each is configured to process the full load of call traffic and network monitoring for the state.

System redundancy – TCS configures its systems for [redacted] [12a] call processing. By designing each system node to distribute traffic in the [redacted] [12a] manner, TCS data centers [redacted] [12a] traffic. [redacted] [12a]

[redacted]



Network redundancy – The STATE will receive system and network monitoring services that are supported by [12a]. Similar diversity and redundancy influence all network build-out aspects.

Software component redundancy – The TCS [12a] supports high availability through the use of redundant software components available to perform the same task, running across multiple servers in multiple locations. TCS incorporates component redundancy in the construction of its [12a] system, combined with both local and geographic redundancy for all production processes, [12a].

2.4.2.2. Availability Responsibilities

Exhibit 66 delineates responsibilities between TCS and MIL for availability.

Exhibit 66. Availability Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
AVAIL-01	Operate the NG9-1-1 functional elements at a 99.999% (“five nines”) availability as measured: Total time in a month, minus any durations of SIL1 or SIL2. If there is no SIL1 or 2, then the service is deemed available	R	
AVAIL-02	Verify the system’s ability to failover from one data center to another with no reduction in service, performance, or availability on an annual basis	R	
AVAIL-03	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.4.2.3. Availability Proposal References

Exhibit 67 lists the applicable proposal and RFP references for availability.

Exhibit 67. Availability Proposal References

Proposal Section #	Proposal Section Title
11.1.11	No Single Point of Failure – [RFP 6.1.11]
11.1.13	Automatic Fail-Over – [RFP 6.1.13]
11.1.14	Shared Infrastructure – [RFP 6.1.14]
11.2.2.1	NLIS Availability – [RFP 6.2.2.1]
7.2.3.1	Availability – [RFP 6.2.3.1]
7.2.4.1	Availability – [RFP 6.2.4.1]
7.2.5.8	Separate SIP Proxy – [RFP 6.2.5.8]
7.2.5.10	Documentation – [RFP 6.2.5.10]
7.2.6.1	Availability – [RFP 6.2.6.1]



Proposal Section #	Proposal Section Title
0	“The current methods supported are a [12a] “make busy” tablet application. This feature is on the roadmap and slated for release [12a] Session Routing – [RFP 6.2.6.7]
7.2.8.2	Availability – [RFP 6.2.8.2]

2.4.3. Performance

2.4.3.1. Performance Description

Performance is defined as the overall, end-to-end NG9-1-1 system’s ability to process incoming calls and maintain a level of call concurrency.

2.4.3.2. Performance Responsibilities

Exhibit 68 delineates responsibilities between TCS and MIL for performance.

Exhibit 68. Performance Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
PERF-01	Provide an NG9-1-1 solution that supports [12a] concurrent calls	R	I
PERF-02	Provide an NG9-1-1 solution that supports up to [12a]	R	
PERF-03	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.4.3.3. Performance Proposal References

Exhibit 69 lists the applicable proposal and RFP references for performance.

Exhibit 69. Performance Proposal References

Proposal Section #	Proposal Section Title
7.2.5.9	Capacity – [RFP 6.2.5.9]
7.2.6.11	Session Processing Capacity – [RFP 6.2.6.11]
7.2.8.7	ECRF Capacity – [RFP 6.2.8.7]

2.4.4. Hardware Compliance

2.4.4.1. Hardware Compliance Description

The NG9-1-1 solution for MIL uses commercial off-the-shelf (COTS) equipment that complies with all appropriate Federal Communications Commission (FCC), Underwriters Laboratories (UL)/Canadian Standards Association (CSA), Conformité Européene (CE), and NENA standards



as they apply to such elements as electrical safety and electromagnetic interference (EMI) for computer and telecommunications equipment.



2.4.4.2. Hardware Compliance Responsibilities

Exhibit 70 delineates responsibilities between TCS and MIL for hardware compliance.

Exhibit 70. Hardware Compliance Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
HARD-01	Ensure all hardware used for the delivery of NG9-1-1 service for MIL conforms to FCC Rules Part 15, Class A (commercial, non-residential radiation and conduction limits) for EMI	R	
HARD-02	Ensure hardware (where applicable) conforms to: UL	R	
HARD-03	Ensure hardware (where applicable) conforms to: International Organization of Standards (ISO)	R	
HARD-04	Ensure hardware (where applicable) conforms to: Institute of Electrical and Electronics Engineers (IEEE)	R	
HARD-05	Ensure hardware (where applicable) conforms to: NENA	R	
HARD-06	Ensure hardware (where applicable) conforms to: American National Standards Institute (ANSI)	R	
HARD-07	Ensure hardware (where applicable) conforms to: Electronic Industries Alliance (EIA)	R	
HARD-08	Ensure hardware (where applicable) conforms to: Telecommunications Industry Association (TIA), (including [12a] Commercial Building Telecommunications Wiring Standards), etc.	R	
HARD-09	Report any noted exceptions		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.4.4.3. Hardware Compliance Proposal References

Exhibit 71 lists the applicable proposal and RFP references for hardware compliance.

Exhibit 71. Hardware Compliance Proposal References

Proposal Section #	Proposal Section Title
11.1.1	Federal Communications Commission (FCC) Rules – [RFP 6.1.1]
11.1.2	Industry Standards – [RFP 6.1.2]

2.4.5. System and Network Monitoring

2.4.5.1. System and Network Monitoring Description

Monitoring is provided by the TCS [12a] (see Exhibit 125), with a fully staffed 24x7 facility in TCS’ [12a].

2.4.5.2. System and Network Monitoring Responsibilities

Exhibit 72 delineates responsibilities between TCS and MIL for System and Network Monitoring.

Exhibit 72. System and Network Monitoring Responsibilities



Reference #	System/Service	Responsibility	
		TCS	MIL
MONITOR-01	Produce the procedures for working with the TCS [12a]	R	I

Legend: “R” Responsible, “T” Informed, “C” Consulted

2.4.5.3. System and Network Monitoring References

Exhibit 73 lists the applicable proposal and RFP references for monitoring.

Exhibit 73. Monitoring Proposal References

Proposal Section #	Proposal Section Title
11.1.12	“365 X 24 X 7” ESInet Monitoring System – [RFP 6.1.12]
11.1.15	Outage Notification – [RFP 6.1.15]
7.3.1.1	Connectivity Monitoring – [RFP 6.3.1.1]

2.4.6. PSAP Abandonment Process

2.4.6.1. PSAP Abandonment Description

[12a]

When a PSAP abandonment decision is made, the PSAP will contact [12a] and provide authentication information before requesting abandonment. The [12a] operator will abandon the facility to the preset abandonment route and notify MIL of the facility condition. The PSAP will coordinate with resources in the field to coordinate a test call to verify the state of the abandoned PSAP, and verify the new routing.

To restore normal operations and unabandon the facility, the PSAP will contact [12a] and provide authentication information before requesting that the PSAP begin receiving calls again. MIL will coordinate with resources in the field to coordinate a test call to verify the state of the PSAP.

Secondary Abandonment – In the event that an authorized representative of the PSAP request that a pre-provisioned, but not primary, abandonment route be invoked, the PSAP will communicate the alternate abandonment route, and [12a] will execute the abandonment to the requested alternate abandonment route. Once complete, the PSAP will coordinate with resources in the field to coordinate a test call to verify the state of the abandoned PSAP and verify the new routing.



2.4.6.2. PSAP Abandonment Responsibilities

Exhibit 74 delineates responsibilities between TCS and MIL/PSAP for PSAP abandonment.

Exhibit 74. PSAP Abandonment Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
ABAND-01	[12a]	I	R
ABAND-02	Contact [12a] with the proper credentials and request the abandonment or reactivation	I	R
ABAND-03	Verify the identity and credentials of the person requesting a PSAP abandonment or reactivation	R	
ABAND-04	Notify [12a] whenever a PSAP abandonment or reactivation occurs	R	
ABAND-05	Create a ticket to track each abandonment and unabandonment request	R	I
ABAND-06	Coordinate the field verification test calls	I	R
ABAND-07	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.4.6.3. PSAP Abandonment Proposal References

Exhibit 75 lists the applicable proposal and RFP references for PSAP Abandonment.

Exhibit 75. PSAP Abandonment Proposal References

Proposal Section #	Proposal Section Title
0	County 911 Authority – [RFP 6.1.19]

2.5. Security

2.5.1. NENA NG-SEC 75-001 Compliance

2.5.1.1. NENA NG-SEC 75-001 Compliance Description

TCS currently complies with NENA’s NG-SEC 75-001 per the compliance matrix in Section 8.

A mutually agreed upon third-party auditor will perform audits [12a] using the NENA NG-SEC 75-502 audit checklist but understands MIL may incorporate additional mutually agreed to metrics to the audit checklist.



2.5.1.2. NENA NG-SEC 75-001 Compliance Responsibilities

Exhibit 76 delineates responsibilities between TCS and MIL for NENA NG-SEC 75-001 compliance.

Exhibit 76. NENA NG-SEC 75-001 Compliance Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
NGSEC-01	Perform security audits for all NG Core Services and related network elements [12] al	R	
NGSEC-02	Review TCS' security audit report and provide feedback [12a] of the report		R
NGSEC-03	Reporting any noted exceptions		R
NGSEC-04	Initial audit shall be performed as part of the ATP.	R	

Legend: "R" Responsible, "I" Informed, "C" Consulted

2.5.1.3. NENA NG-SEC 75-001 Compliance Proposal References

Exhibit 77 lists the applicable proposal and RFP references for NENA NG-SEC 75-001.

Exhibit 77. NENA NG-SEC 75-001 Proposal References

Proposal Section #	Proposal Section Title
7.2.13.3.1	NENA NG-SEC 75-001 – [RFP 6.2.13.1]
7.2.13.3.1	Third-Party Security Audit(s) Basis – [RFP 6.2.13.3.1]

2.5.2. Washington OCIO Policy Compliance

2.5.2.1. Washington OCIO Policy Compliance Description

TCS currently complies with MIL's Office of the Chief Information Officer (OCIO) policy per the compliance matrix in Section 8.

A mutually agreed upon THIRD PARTY auditor will perform audits on a [12a] using a mutually agreed upon scope of audit requirements. TCS will make available the Security Audit for review.

2.5.2.2. Washington OCIO Policy Compliance Responsibilities

Exhibit 78 delineates responsibilities between TCS and MIL for Washington OCIO policy compliance.

Exhibit 78. Washington OCIO Policy Compliance Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
OCIO-01	Perform security audits [12a]	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
OCIO-02	Review TCS' security audit report and provide feedback [12a] of the report		R
OCIO-03	Report any noted exceptions		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

2.5.2.3. Washington OCIO Policy Compliance Proposal References

Exhibit 79 lists the applicable proposal and RFP references for Washington OCIO policy compliance.

Exhibit 79. Washington OCIO Policy Compliance Proposal References

Proposal Section #	Proposal Section Title
7.2.13.2	OCIO Policy 141.10 – [RFP 6.2.13.2]
7.2.13.3	Independent Third-Party Security, Availability, and Confidentiality Audits – [RFP 6.2.13.3]

2.6. Standards Compliance

This section addresses compliance with NENA 08-751 and NENA 08-003.

Exhibit 80 lists the applicable proposal and RFP references for global ESInet compliance.

Exhibit 80. Standards Compliance Proposal References

Proposal Section #	Proposal Section Title
8	Global ESInet Requirements [RFP 6.1]

2.6.1. NENA 08-751 Compliance

2.6.1.1. NENA 08-751 Compliance Description

TCS currently complies with the NENA 08-751 per the compliance matrix in Section 10.

2.6.1.2. NENA 08-751 Compliance Responsibilities

Exhibit 81 delineates responsibilities between TCS and MIL for NENA 08-751 compliance.

Exhibit 81. NENA 08-751 Compliance Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
NENAI3-01	Provide software updates that meet the NENA 08-751 requirements within the duration of the contract	R	
NENAI3-02	Provide software enhancements in accordance to the NENA 08-751 for the software changes necessary to fulfill the NGCS-related requirements within the term of the CONTRACT.	R	
NENAI3-03	Provide an annual roadmap of availability for future NENA 08-751 functionality	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
NENAI3-04	Report any noted exceptions.		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.6.1.3. NENA 08-751 Compliance Proposal References

Exhibit 82 lists the applicable proposal and RFP references for NENA 08-751 compliance.

Exhibit 82. NENA 08-751 Compliance Proposal References

Proposal Section #	Proposal Section Title
7.2.6.10	Issue SIP NOTIFY – [RFP 6.2.6.10]
7.2.14	Basic Call Processing – [RFP 6.2.14]

2.6.2. NENA i3 [08-003] Compliance

2.6.2.1. NENA i3 [08-003] Compliance Description

TCS currently complies with the NENA 08-003 per the compliance matrix in Section 11.

2.6.2.2. NENA i3 [08-003] Compliance Responsibilities

Exhibit 83 delineates responsibilities between TCS and MIL for NENA i3 [STA 010/08-003] compliance.

Exhibit 83. NENA i3 [08-003] Compliance Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
NENASTA-01	Provide software updates that meet the NENA i3 requirements within the duration of the contract	R	
NENASTA-02	Provide software enhancements in accordance to the NENA STA010 for the software changes necessary to fulfill the NGCS-related requirements within the term of the CONTRACT.	R	
NENASTA-03	Provide an annual roadmap of availability for future NENA i3 functionality	R	
NENASTA-04	Report any noted exceptions		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.6.2.3. NENA i3 [08-003] Compliance Proposal References

Exhibit 84 lists the applicable proposal and RFP references for NENA i3 [STA 010/08-003] compliance.

Exhibit 84. NENA i3 [08-003] Compliance Proposal References

Proposal Section #	Proposal Section Title
11.1.4	IP Compliance – [RFP 6.1.4]



Proposal Section #	Proposal Section Title
7.2.8.1	ECRF NENA – [RFP 6.2.8.1]

2.7. Other Options Selected from the RFP

2.7.1. LNG(s) to ESRP

2.7.1.1. LNG(s) to ESRP Description

A PSTN gateway is part of the solution. [12a]

[REDACTED]

[REDACTED]

[REDACTED] A log of the default routing action will be generated and acted upon to resolve the problem.

2.7.1.2. LNG(s) to ESRP Responsibilities

Exhibit 85 delineates responsibilities between TCS and MIL for LNG(s) to ESRP services.

Exhibit 85. LNG(s) to ESRP Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
LNGESRP-01	If, after re-attempting the call, a “200 OK” or a “486 Busy Here” message is still not received for the call, an alarm shall be raised and the root cause will be investigated.	R	
LNGESRP-02	In the scenario above, [12a] provide alternate routing information to route the call to the PSTN Gateway as follows: <ul style="list-style-type: none"> LNG will re-attempt the call to the other ESRP(s) – including the georedundant ESRPs and the other georedundant LNG. If the georedundant ESRP(s) also fail to respond, then the LNG must [12a] 	R	I
LNGESRP-03	Configure this feature on a PSAP basis with a default setting of OFF.	R	I
LNGESRP-04	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.7.1.3. LNG(s) to ESRP Proposal References

Exhibit 86 lists the applicable proposal and RFP references for LNG(s) to ESRP.

Exhibit 86. LNG(s) to ESRP Proposal References

Proposal Section #	Proposal Section Title
7.2.15.1	LNG(s) to ESRP – [RFP 6.2.15.1]



2.7.2. ESRP PSTN Gateway Routing

2.7.2.1. ESRP PSTN Gateway Routing Description

A PSTN gateway is part of the solution. [12a]

A log of the default routing action will be generated and acted upon to resolve the problem.

2.7.2.2. ESRP PSTN Gateway Routing Responsibilities

Exhibit 87 delineates responsibilities between TCS and MIL for ESRP PSTN gateway routing.

Exhibit 87. LNG(s) to ESRP Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
ESRPPSTN-01	If, after re-attempting the call, a "200 OK" or a "486 Busy Here" message is still not received for the call, an alarm shall be raised and the root cause will be investigated.	R	
ESRPPSTN-02	In the scenario above, the ESRP/PRF will provide alternate routing information to route the call to the PSTN Gateway as follows: <ul style="list-style-type: none"> [12a] 	R	I
ESRPPSTN-03	[12a]	R	I
ESRPPSTN-04	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

2.7.2.3. ESRP PSTN Proposal References

Exhibit 88 lists the applicable proposal and RFP references for ESRP PSTN.

Exhibit 88. ESRP PSTN Proposal References

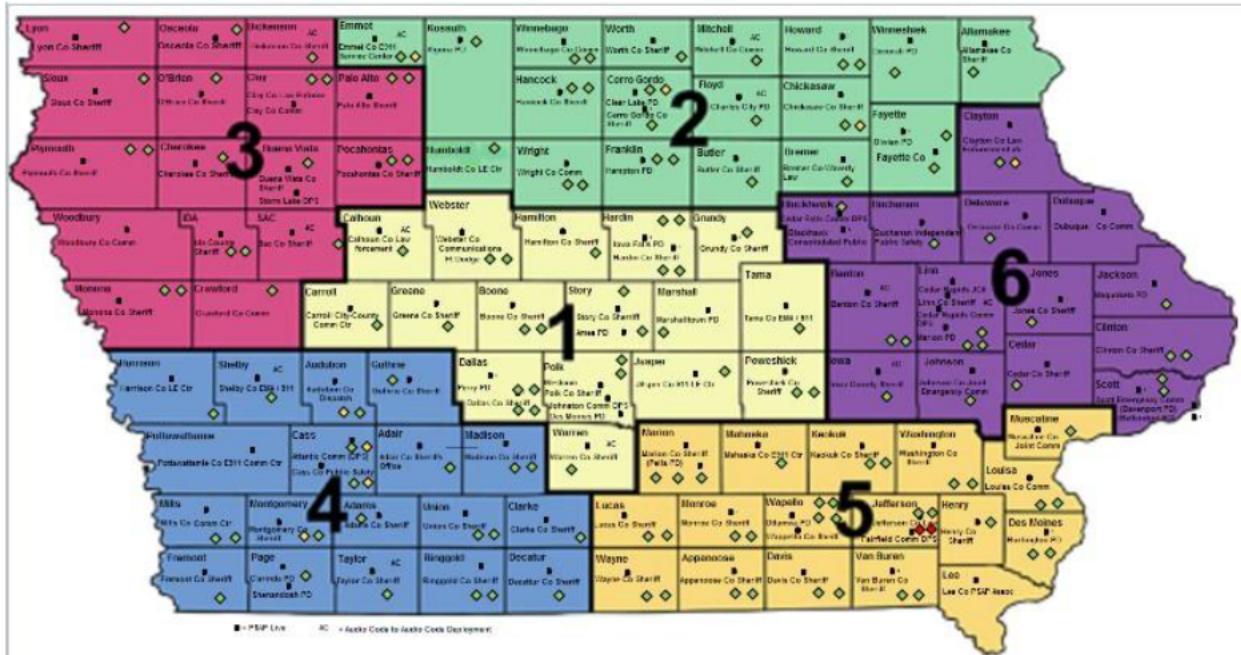
Proposal Section #	Proposal Section Title
7.2.15.3	ESRP PSTN Gateway Routing – [RFP 6.2.15.3]

2.7.3. Monitoring Dashboard

The monitoring dashboard will have a map of the State of Washington similar to the image below.



Washington State Military Department
 Next Generation 9-1-1 Emergency Services Internet Protocol Network
 Statement of Work | June 24, 2016



TCS will provide a product description of the monitoring dashboard 120 days after project kickoff.

2.7.3.1. Monitoring Dashboard Description

This section addresses the optional monitoring dashboard requirements from Section 6.2.22 of the RFP.

2.7.3.2. Monitoring Dashboard Responsibilities

Exhibit 89 delineates responsibilities between TCS and MIL for monitoring dashboard services.

Exhibit 89. Monitoring Dashboard Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
DASH-01	Provide [12a]	R	
DASH-02	Provide the list of named users and credentials	I	R
DASH-03	Support the client browser [12a]	R	
DASH-04	Support drill down on relevant network elements in the monitoring dashboard	R	
DASH-05	Use a green, yellow, red color scheme to indicate operational states of fully operational, non-call affecting problem, call delivery affecting problem.	R	
DASH-06	Provide a monitoring system with a refresh rate [12a]	R	
DASH-07	Provide a GUI network element monitoring system that monitors connectivity and functional elements of the STATE of Washington ESInet	R	
DASH-08	Provide a product description [12a] after project kickoff and MIL will sign off on these product requirements	R	I



Reference #	System/Service	Responsibility	
		TCS	MIL
DASH-09	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.7.3.3. Monitoring Dashboard Proposal References

Exhibit 90 lists the applicable proposal and RFP references for the monitoring dashboard.

Exhibit 90. Monitoring Dashboard Proposal References

Proposal Section #	Proposal Section Title
7.2.22.1	Network Monitoring Dashboard – [RFP 6.2.22.1]
7.2.22.2	Graphical Display – [RFP 6.2.22.2]
7.2.22.3	Near-Real Time Display – [RFP 6.2.22.3]
7.2.22.4	Operational States – [RFP 6.2.22.4]
7.2.22.5	Display Drill-Down – [RFP 6.2.22.5]
7.2.22.6	Dashboard Access – [RFP 6.2.22.6]
7.2.22.7	Browser – [RFP 6.2.22.7]

2.7.4. PSTN Gateway

2.7.4.1. PSTN Gateway Description

A PSTN gateway is part of the solution. [12a]
 [Redacted]
 [Redacted]
 [Redacted] A log of the default routing action will be generated and acted upon to resolve the problem.

2.7.4.2. PSTN Gateway Responsibilities

Exhibit 91 delineates responsibilities between TCS and MIL for PSTN gateway services.

Exhibit 91. PSTN Gateway Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
PSTNGW-01	In the event that an ESRP cannot deliver a call to a PSAP (primary, backup, default) served by the ESnet, the ESRP shall: <ul style="list-style-type: none"> [Redacted] [12a] [Redacted] [Redacted] or 	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
	<ul style="list-style-type: none"> [12a] 		
PSTNGW-02	This feature shall be settable on a per-PSAP basis with [12a]	R	
PSTNGW-03	If this occurs, an alarm will be raised indicating that a 9-1-1 call could not be terminated via the ESInet and the root cause will be investigated.	R	
PSTNGW-04	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.7.4.3. PSTN Gateway Proposal References

Exhibit 92 lists the applicable proposal and RFP references for the PSTN gateway.

Exhibit 92. PSTN Gateway Proposal References

Proposal Section #	Proposal Section Title
7.2.10	PSTN Gateway(s) – [RFP 6.2.10]

2.7.5. Callback Numbers for Failed Calls

2.7.5.1. Callback Numbers for Failed Calls Description

TCS will provide a report for MIL that identifies the CBN of wireline, VoIP i2, and wireless calls for calls identified in the Failed Calls report. The CBNs related to p-ANIs will only be from the carriers supported by the TCS MPC/GMLC/VPC. For carriers not serviced by a TCS MPC/GMLC/VPC, TCS will make a reasonable effort to retrieve the CBN for failed calls from these carriers and/or their service providers. MIL may be required to provide a formal request/letter of authority to TCS (or otherwise authorize TCS in writing) to act on behalf of MIL in order to retrieve the CBN for call failures from carriers and/or their service providers.

2.7.5.2. Callback Numbers for Failed Calls Responsibilities

Exhibit 93 delineates responsibilities between TCS and MIL for CBNs for failed call services.

Exhibit 93. Call Back Numbers for Failed Calls Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
CBN-01	Provide a report for MIL that identifies the CBN for VoIP i2 and wireless calls using the Failed Calls Report. These CBNs will only be from carriers supported by the TCS MPC/GMLC/VPC.	R	
CBN-02	Email this report to a MIL-identified email address.	R	I
CBN-03	Confirm receipt of the report.	I	R



Reference #	System/Service	Responsibility	
		TCS	MIL
CBN-04	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

2.7.5.3. Callback Numbers for Failed Calls Proposal References

Exhibit 94 lists the applicable proposal and RFP references for CBNs for failed calls.

Exhibit 94. Call-Back Numbers for Failed Calls Proposal References

Proposal Section #	Proposal Section Title
11.1.17	Call Back Numbers for Failed Calls – [RFP 6.1.17]

2.7.6. Callback Number System

2.7.6.1. Callback Number System Description

TCS will provide [12a] [REDACTED] for MIL that replaces the CBN report from Section 2.7.5 which identifies the CBN of wireline, VoIP i2 and wireless calls for calls identified in the Failed Calls report. The CBNs provided will only be from the carriers supported by the TCS MPC/GMLC/VPC. The CBNs related to p-ANIs will only be from the carriers supported by the TCS MPC/GMLC/VPC. For carriers not serviced by a TCS MPC/GMLC/VPC, TCS will make a reasonable effort to retrieve the CBN for failed calls from these carriers and/or their service providers. MIL may be required to provide a formal request/letter of authority to TCS (or otherwise authorize TCS in writing) to act on behalf of MIL in order to retrieve the CBN for call failures from carriers and/or their service providers.

2.7.6.2. Callback Number System Responsibilities

Exhibit 95 delineates responsibilities between TCS and MIL for Callback Number System services.

Exhibit 95. Callback Number System Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
CBNS-01	Provide a web portal for access by PSAPs and MIL to the list of CBNs for calls identified on the Failed Calls report	R	
CBNS-02	Provide this [12a] [REDACTED] of project kickoff	R	
CBNS-03	Provide the list and credentials of users requiring access	I	R
CBNS-04	Accurate and timely trouble reporting and description of problems to TCS [12a] [REDACTED] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted



2.7.6.3. Callback Number System Proposal References

Exhibit 96 lists the applicable proposal and RFP references for the Callback Number System.

Exhibit 96. Call-Back Number System Proposal References

Proposal Section #	Proposal Section Title
11.1.18	Call Back Number System – [RFP 6.1.18]



3. Network

3.1. General Networking

3.1.1.1. General Networking Description

Due to the nature and the number of disparate software and hardware components in an ESInet, the most efficient and effective IP routing solution requires a network that simultaneously supports IP version 4 (IPv4) and IP version 6 (IPv6) in its addressing and routing (that is, a “dual-stack” approach). To that end, the proposed TCS solution includes software services and network components that can be configured to support both IPv4 and IPv6.

For MOS compliance, TCS uses [12a] method of determining MOS through network-based appliances.

3.1.1.2. General Networking Responsibilities

Exhibit 97 delineates responsibilities between TCS and MIL for general networking.

Exhibit 97. General Networking Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
GENNET-01	Maintain an average MOS of [12a]	R	I
GENNET-02	Measure and report MOS	R	I
GENNET-03	Ensure the bandwidth ordered for each PSAP [12a]	R	
GENNET-04	[12a] voice call to the PSAP	R	
GENNET-05	Operate the network with the dual-stack approach for IPv4/IPv6	R	

Legend: “R” Responsible, “I” Informed, “C” Consulted

3.1.1.3. General Networking Proposal References

Exhibit 98 lists the applicable proposal and RFP references for general networking.

Exhibit 98. General Networking Proposal References

Proposal Section #	Proposal Section Title
11.1.3	Support for IPv4 and IPv6 – [RFP 6.1.3]
11.1.7	Bandwidth per Audio Session (Call) – [RFP 6.1.7]
11.1.8	Call Quality – [RFP 6.1.8]
11.1.9	Guaranteed Bandwidth (Hard QoS) – [RFP 6.1.9]
7.2.5.5	TCP – [RFP 6.2.5.5]



3.2. TCS MPLS Network

3.2.1. TCS MPLS Network Description

TCS uses its [12a] MPLS networks to support redundant access for the purpose of managing and monitoring services provided to MIL in TCS data centers, and for transporting [12] signaling from the [12a] to the LNG/PIF.

The MPLS network(s) used by TCS provides the following:

- Network path from the TCS [12a] to the LNG-LSRG/PIF
- Network path for TCS support engineers
- Network path for TCS [12a] monitoring

3.2.2. TCS MPLS Network Responsibilities

Exhibit 99 delineates responsibilities between TCS and MIL for TCS MPLS network services.

Exhibit 99. TCS MPLS Network Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
MPLSTC-01	Acquire, install, and maintain connectivity between TCS data centers and MIL PSAPs	R	

Legend: “R” Responsible, “T” Informed, “C” Consulted

3.3. ESInet MPLS Network

3.3.1. ESInet MPLS Network Description

The [12a] MPLS network(s) used as part of the ESInet provides the following:

- [12a]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

3.3.2. ESInet MPLS Network Responsibilities

Exhibit 100 delineates responsibilities between TCS and MIL for ESInet MPLS network services.



Exhibit 100. ESInet MPLS Network Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
MPLSES-01	Acquire, install, and maintain connectivity between TCS data centers and MIL PSAPs	R	I
MPLSES-02	[12a] per voice call between the TCS data centers and MIL PSAPs	R	
MPLSES-03	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

3.3.3. ESInet MPLS Network Proposal References

Exhibit 101 lists the applicable proposal and RFP references for ESInet MPLS.

Exhibit 101. ESInet MPLS Proposal References

Proposal Section #	Proposal Section Title
7.2.4.11	BCF (Terminating) to PSAP Connectivity – [RFP 6.2.4.11]
7.2.19.1	ESInet PSAP – [RFP 6.2.19.1]

3.4. TDM

3.4.1. Voice [12a] TDM

3.4.1.1. Voice [12a] TDM Description

TDM is required in this solution for the ingress from the originating service provider(s) and inter-tandem trunks from SRs.

- Logical routesets [12a] between an SR and the TCS STP pair
- Logical routesets [12a] between an originating service provider at the TCS STP pair
- Physical circuits/connections for voice between the LSRG-PIF and an SR
- Physical circuits/connections for voice between the LNG-PIF and an originating service provider

3.4.1.2. Voice [12a] TDM Responsibilities

Exhibit 102 delineates responsibilities between TCS and MIL for ESInet MPLS network services.

Exhibit 102. Voice [12a] Responsibilities



Reference #	System/Service	Responsibility		
		TCS	MIL	CSP
TDMSS7-01	Acquire, install, and maintain connectivity (voice [12a]) to SRs while necessary	R		I
TDMSS7-02	Install and maintain CSP connectivity at the LNG/PIF.	R		
TDMSS7-03	Acquire, install, and maintain connectivity (voice [12a]) to the LNG-PIF			R
TDMSS7-04	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R	

Legend: “R” Responsible, “I” Informed, “C” Consulted

3.4.1.3. Voice [12a] TDM Proposal References

Exhibit 103 lists the applicable proposal and RFP references for voice [12a] services.

Exhibit 103. TDM Proposal References

Proposal Section #	Proposal Section Title
7.2.19.2	ESInet-Originating Network Connectivity – [RFP 6.2.19.2]

3.5. Media (Voice/Text/Video)

3.5.1. Voice Services

3.5.1.1. Voice Services Description

Audio is converted by the TCS LNG/LSRG-PIF from TDM ingress trunks. Audio is routed using SIP and delivered using RTP. Audio is also supported as a direct SIP/RTP connection through the BCF for MIL-approved and ESInet-supported external IP connections.

- Audio (RTP) is [12a].
- All RTP will use [12a].
- All SIP will use [12a] across the ESInet.
- All RTP will use [12a] across the ESInet.

[12a]

3.5.1.2. Voice Services Responsibilities

Exhibit 104 delineates responsibilities between TCS and MIL for voice services.

Exhibit 104. Voice Services Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
VOICE-01	Convert TDM to SIP/RTP from carrier and inter-tandem trunks [12a]	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
VOICE-02	Convert SIP/RTP from the ESInet to TDM at the PSAP via the installed LPG-PIF	R	
VOICE-03	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

3.5.2. Text Services

3.5.2.1. Text Services Description

Text is routed using SIP and delivered using MSRP.

- Text messages using MSRP as the transport are delivered into the MIL ESInet from TCC providers [12a]
- Media (MSRP) are [12a].
- Support transfer requests from PSAPs for text-to-911 messages once the standard has been determined and approved.

3.5.2.2. Text Services Responsibilities

Exhibit 105 delineates responsibilities among TCS, MIL, and CSP for text services.

Exhibit 105. Text Services Responsibilities

Reference #	System/Service	Responsibility		
		TCS	MIL	CSP
TEXT-01	[12a]	I		R
TEXT-02	Establish interconnectivity with TCC vendors as requested by the State	R		
TEXT-03	Define the text-to-911 bounceback message	I	R	
TEXT-04	Provide bounceback messages to the sending TCC when text-to-911 service is not available for that inbound session request	R	I	
TEXT-05	Route to destination PSAPs based on lat/lon of the session request and the routing policies established by MIL	R	I	
TEXT-06	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R	

Legend: "R" Responsible, "I" Informed, "C" Consulted

3.5.2.3. Text Services Proposal References

Exhibit 106 lists the applicable proposal and RFP references for text services.



Exhibit 106. Text Services Proposal References

Proposal Section #	Proposal Section Title
7.2.4.6	Text Support – [RFP 6.2.4.6]
7.2.4.7	Text Control Center (TCC) Integration – [RFP 6.2.4.7]

3.5.3. Video Services

3.5.3.1. Video Services Description

TCS supports the pass-through routing of H.264/MPEG-4 streaming video. Other video codecs will be supported as standards bodies agree on implementation details.

3.5.3.2. Video Services Responsibilities

Exhibit 107 delineates responsibilities between TCS and MIL for video services.

Exhibit 107. Video Services Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
VIDEO-01	Support the pass-through routing of H.264/MPEG-4 streaming video to PSAPs using the ESRP/PRF	R	
VIDEO-02	Coordinate testing with CPE providers able to support H.264/MPEG-4 streaming video	I	R
VIDEO-03	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

3.5.3.3. Video Services Proposal References

Exhibit 108 lists the applicable proposal and RFP references for video services.

Exhibit 108. Video Services Proposal References

Proposal Section #	Proposal Section Title
7.2.4.8	Video CODEC Support – [RFP 6.2.4.8]



4. Interconnection

4.1. SIP and i3-Compliant CPE Interconnection

4.1.1. SIP and i3-Compliant CPE Interconnection Description

This SOW supports connection from the TCS provided MIL ESInet to direct IP-connected PSAPs using the NENA i3 specification or the RFAI version specified in the CPE interface specification. TCS will provide an interface specification for IP-enabled CPE providers to follow [12a]

4.1.2. SIP and i3-Compliant CPE Interconnection Responsibilities

Exhibit 109 delineates responsibilities between TCS and MIL for i3-compliant CPE interconnection.

Exhibit 109. SIP and i3-Compliant CPE Interconnection Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
CPE-01	Maintain the SIP interworking specification that communicates the available standard interfaces (NENA i3 and RFAI) to CPE providers for SIP and i3 connectivity	R	
CPE-02	Deliver the SIP interworking specification to CPE providers that do business in the STATE of Washington		R
CPE-03	Deploy and manage the specified routers for direct IP connectivity	R	
CPE-04	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: “R” Responsible, “I” Informed, “C” Consulted

4.1.3. SIP and i3-Compliant CPE Interconnection Proposal References

Exhibit 110 lists the applicable proposal and RFP references for video services.

Exhibit 110. Video Services Proposal References

Proposal Section #	Proposal Section Title
11.1.5	SIP Interface Specification – [RFP 6.1.5]

4.2. Interconnection with ALI Database(s)

4.2.1. Interconnection with ALI Databases Description

Location and caller information is retrieved from ALI database(s) using the LNG/LIF function. ALI database connections will use [12a]



[12a] TCS will provide a copy of this document.

4.2.2. Interconnection with ALI Databases Responsibilities

Exhibit 111 delineates responsibilities between TCS and MIL for interconnection with ALI databases.

Exhibit 111. Interconnection with ALI Databases Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
INTALI-01	Establish connectivity to ALI databases serving PSAP in the STATE of Washington	R	
INTALI-02	Provide letter of authorization to the ALI database providers as required	I	R
INTALI-03	Monitor and maintain connectivity	R	
INTALI-04	Accurate and timely trouble reporting and description of problems to TCS [12a] for events where TCS has no visibility, per established reporting procedures		R

Legend: "R" Responsible, "I" Informed, "C" Consulted

4.3. Interconnection with Dynamic ALI Database(s)

4.3.1. Interconnection with Dynamic ALI Database(s) Description

Location and caller information is retrieved from MPC/GMLC/VPC database(s) using the LNG/LIF function. MPC/GMLC connections will be via the J-STD-036 E2+ interface. Connection to VPCs will be via V-E2.

4.3.2. Interconnection with Dynamic ALI Database(s) Responsibilities

Exhibit 112 delineates responsibilities among TCS, MIL, and CSP for interconnection with dynamic ALI databases.

Exhibit 112. Interconnection with Dynamic ALI Database(s) Responsibilities

Reference #	System/Service	Responsibility		
		TCS	MIL	xPC ¹
INTDALI-01	Acquire, install, and maintain connectivity to the LNG-LIF for access to the dynamic ALI database			R
INTDALI-02	Provide connectivity to MPC/GMLC/VPC dynamic ALI databases serving PSAPs in the STATE of Washington	R		
INTDALI-03	Provide letter of authorization to the MPC/GMLC/VPC dynamic ALI database providers as required	I	R	
INTDALI-04	Monitor connectivity	R		

¹ xPC refers to MPC/GMLC/VPC providers like TCS, West, Sprint and T-Mobile.



Washington State Military Department
 Next Generation 9-1-1 Emergency Services Internet Protocol Network
 Statement of Work | June 24, 2016

Reference #	System/Service	Responsibility		
		TCS	MIL	xPC ¹
INTDALI-05	Accurate and timely trouble reporting and description of problems to TCS [12a], for events where TCS has no visibility, per established reporting procedures		R	

Legend: "R" Responsible, "I" Informed, "C" Consulted



5. Implementation

5.1. Implementation Description

TCS is committed to providing project management services to manage both its internal resources and any external partner and their resources. It is the project manager's job to ensure a successful deployment from the initial kickoff meeting through customer hand-off to TCS' operational account management and steady state operational teams. Project management at TCS starts with a methodology built around Project Management Institute (PMI) standards and then modified to accommodate the unique requirements of each customer. The team will appropriately scale the paperwork methodology so as not to unduly impact the overall project delivery while still conforming to the spirit of the standards established by PMI. Projects at TCS follow internal ISO requirements that detail specific TCS process steps and the artifacts that must be maintained throughout the project lifecycle.

5.2. Implementation Responsibilities

Exhibit 113 delineates responsibilities between TCS and MIL for implementation.

Exhibit 113. Implementation Responsibilities

Reference #	System/Service	Responsibility	
		TCS	MIL
IMP-01	Assign a full-time project manager.	R	I
IMP-02	Conduct and attend recurring project status meetings (both on- and off-site).	R	I
IMP-03	Define roles that are the responsibility of TCS, the State, PSAP, local telephone company, and any SUBCONTRACTORS.	R	C
IMP-04	Manage all network-related change requests.	R	I
IMP-05	Submit written change requests using TCS change request form.	I	R
IMP-06	Submit quotes within 5 business days for change requests.	R	I
IMP-07	Respond to submitted quotes within 10 business days.	I	R
IMP-08	Coordinate with other TCS departments and disciplines.	R	
IMP-09	Develop PROJECT PLANS, schedules, and budgets.	R	C
IMP-10	Review and approve/reject/modify changes to project schedules.		R
IMP-11	Ensure compliance and completion of assigned project tasks.	R	I
IMP-12	Provide written acceptance of completed milestones.		R
IMP-13	Prepare written reports to MIL project point of contact (POC) on all project-related matters.	R	I
IMP-14	At least 1 business day before each meeting, TCS' Project Manager shall create and distribute to all meeting participants a meeting agenda, and present to the STATE a detailed PROGRESS REPORT related to the testing and cutover SERVICES, as applicable.	R	I
IMP-15	The PROGRESS REPORTS shall contain one or more of the following items:	R	



Reference #	System/Service	Responsibility	
		TCS	MIL
	<ul style="list-style-type: none"> Progress on the ACCEPTANCE TEST PLAN (ATP) and/or CUTOVER PLAN since the last PROGRESS REPORT; A summary, in such detail as MIL reasonably requests, of the accomplishments and difficulties encountered, along with suggestions and proposed actions for dealing with and resolving any identified difficulties and the anticipated results; A comprehensive and consolidated log of all outstanding problems and RISKS identified by MIL and/or TCS that remain to be resolved; A comprehensive list of all tasks/activities accomplished and DELIVERABLES completed since the last PROGRESS REPORT; and Any other items as set forth in the ATP and/or CUTOVER PLAN and any other items as MIL reasonably may request of TCS. 		
IMP-16	Produce change order form for MIL's review and approval.	R	I
IMP-17	With respect to change orders submitted to the VENDOR by MIL, the VENDOR shall provide its response within 3 business days (for a simple change request) and within 10 business days (for a complex change request).	R	

Legend: "R" Responsible, "I" Informed, "C" Consulted

5.3. Project Management

TCS' Project Manager shall be dedicated to MIL for the duration of the implementation project and for a period of one month following the date of final acceptance of the system to ensure the system is stable, complies with the details of the contract, and meets all applicable performance and service level guarantees. After this one-month period following initial implementation, TCS will assign an Account Manager as the POC for the State. The Account Manager may or may not be on-site.

TCS' Project Manager may be certified under the PMI Project Management Professional (PMP) program, have an equivalent degree program, or have significant experience in project management. Senior management of the project management staff associated with this project will maintain PMP certification throughout the duration of the project.

Until final acceptance of the system, TCS and MIL shall meet weekly to discuss the status of the solution testing and cutover services, including progress on the ATP and CUTOVER PLAN (including, as applicable, the PSAPs). TCS' Project Manager shall keep minutes of such meetings in a form reasonably satisfactory to MIL and shall provide copies of the minutes to all meeting attendees as soon as reasonably possible, but no later than two business days following each meeting.

TCS' Project Manager shall include in the PROGRESS REPORTS any delays by, or problems or RISKS related to, MIL, TCS, ORIGINATING NETWORKS, PSAPs, and other third parties.

The STATE shall have the right to assume that TCS is not aware of any problems or RISKS or delays unless TCS specifically identifies them in a PROGRESS REPORT.



No problem or RISK shall be deleted or removed from a PROGRESS REPORT until such problem or RISK has been resolved to the State's reasonable satisfaction and MIL agrees to remove the problem or RISK from the PROGRESS REPORT.

5.3.1. Implementation Plan

As part of the project planning, TCS will provide detailed PROJECT PLANS, site survey results, ATPs, and as-built diagrams.

Prior to beginning each phase, the project team will hold a joint detailed planning session. During this planning session a detailed project schedule will be created, roles and responsibilities will be defined by task, and design meetings will be established for the next phase.

Although the product of each phase is dependent on completing the prior phase, TCS plans to overlap work on each phase in a manner that streamlines the schedule, enabling the quickest path to project delivery.

5.3.2. Critical Milestones

The Critical Milestones are set forth in Section 2.6.2 of the Contract.

5.3.3. CPE Compatibility Testing

VENDOR shall schedule and test one (1) PSAP for each CPE type/vendor and provide complete test results for MIL approval before proceeding with connectivity to other PSAPs of the same CPE type/provider.

5.4. Acceptance Test Plan

The ATP for the project is provided as a separate document.

5.5. Implementation Proposal References

Exhibit 114 lists the applicable implementation proposal and RFP references.

Exhibit 114. Implementation Proposal References

Proposal Section #	Proposal Section Title
11.1.20	Implementation Timeline(s) – [RFP 6.1.21]
7.4	Facilitating Carrier Transition – [RFP 6.4]
7.4.1	Conversion of Legacy (CAMA) PSAPs – [RFP 6.4.1]
11.1.6	Existing SIP Compatibility – [RFP 6.1.6]
11.1.21	Acceptance Test Plan (ATP) – [RFP 6.1.22]



Exhibit 115 has been removed from this document.

Exhibit 115. Omitted



6. Supported Call Flows

6.1. Summary of Supported Call Flows

Sections 6.2 through 6.10 illustrate the following types of call flows:

- Call Origination via LSRG – ESN Routed
- Call Origination via LNG – ESN Routed
- Call Origination via BCF – ESN Routed
- Call Origination via LNG – Location (ECRF) Routed
- Call Origination via BCF – Location (ECRF) Routed
- Call Transfer from an LPGCAMA PSAP
- Call Transfer from an LPGRFAI PSAP
- Call Transfer from an i3 PSAP
- Call Transfer – “Figure 4” references General Conferencing



6.2. Call Origination via LSRG – ESN Routed

[12a]



Exhibit 116. Call Origination via LSRG – ESN Routed



6.3. Call Origination via LNG – ESN Routed

[12a]

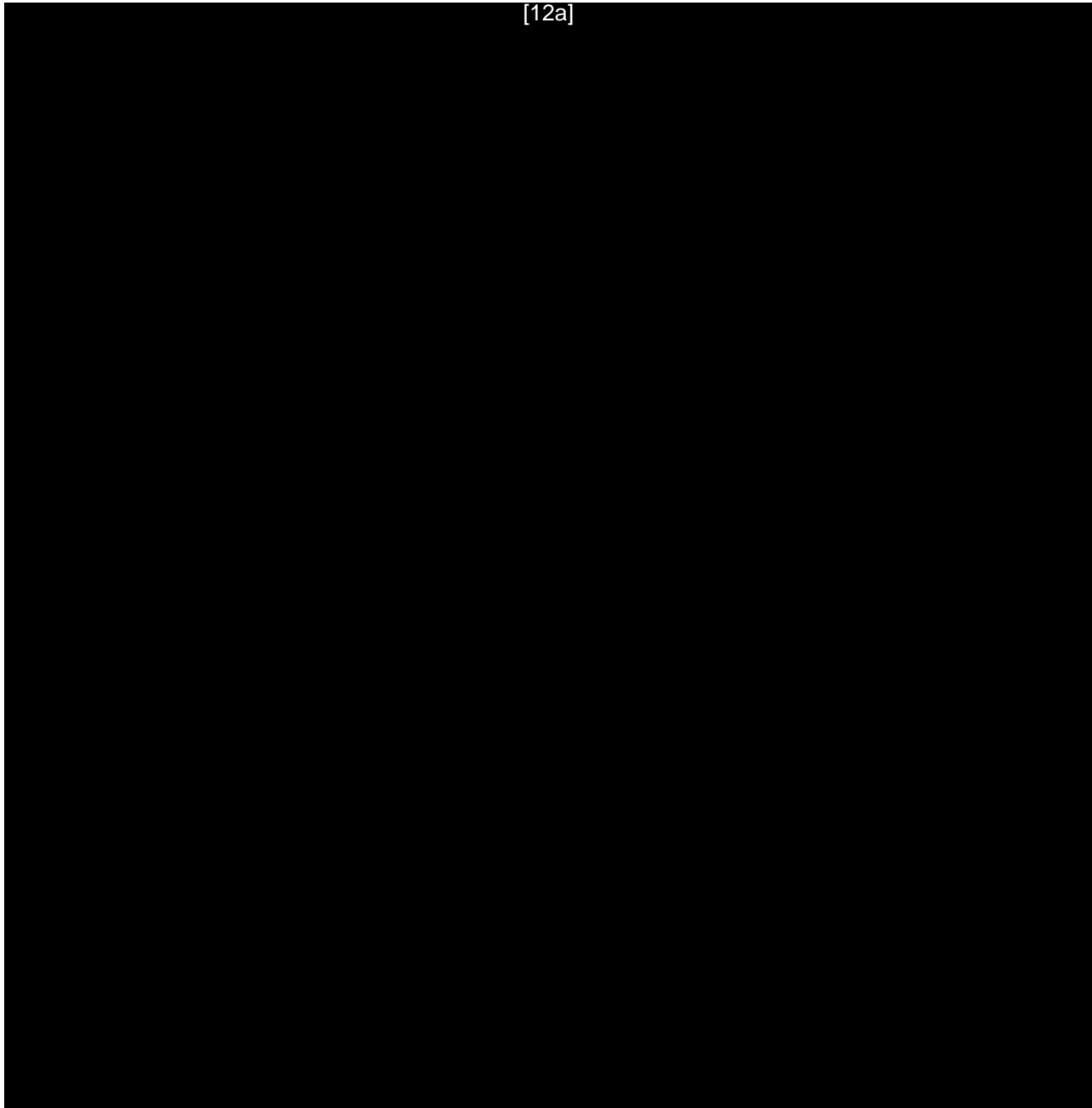


Exhibit 117. Call Origination via LNG – ESN Routed



6.4. Call Origination via BCF – ESN Routed

[12a]

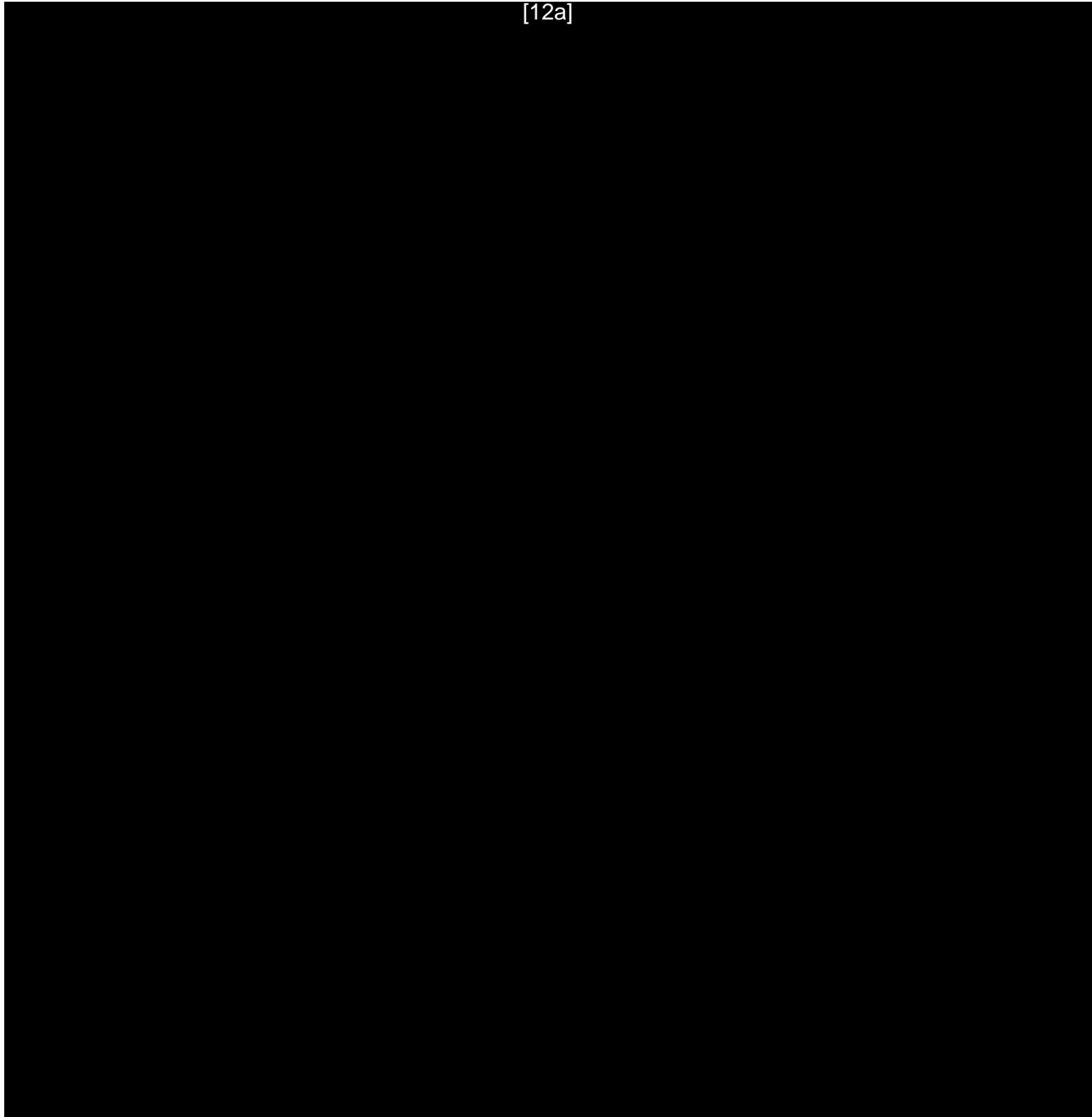


Exhibit 118. Call Origination via BCF – ESN Routed



6.5. Call Origination via LNG – Location Routed

[12a]



Exhibit 119. Call Origination via LNG – Location Routed



6.6. Call Origination via BCF – Location Routed

[12a]

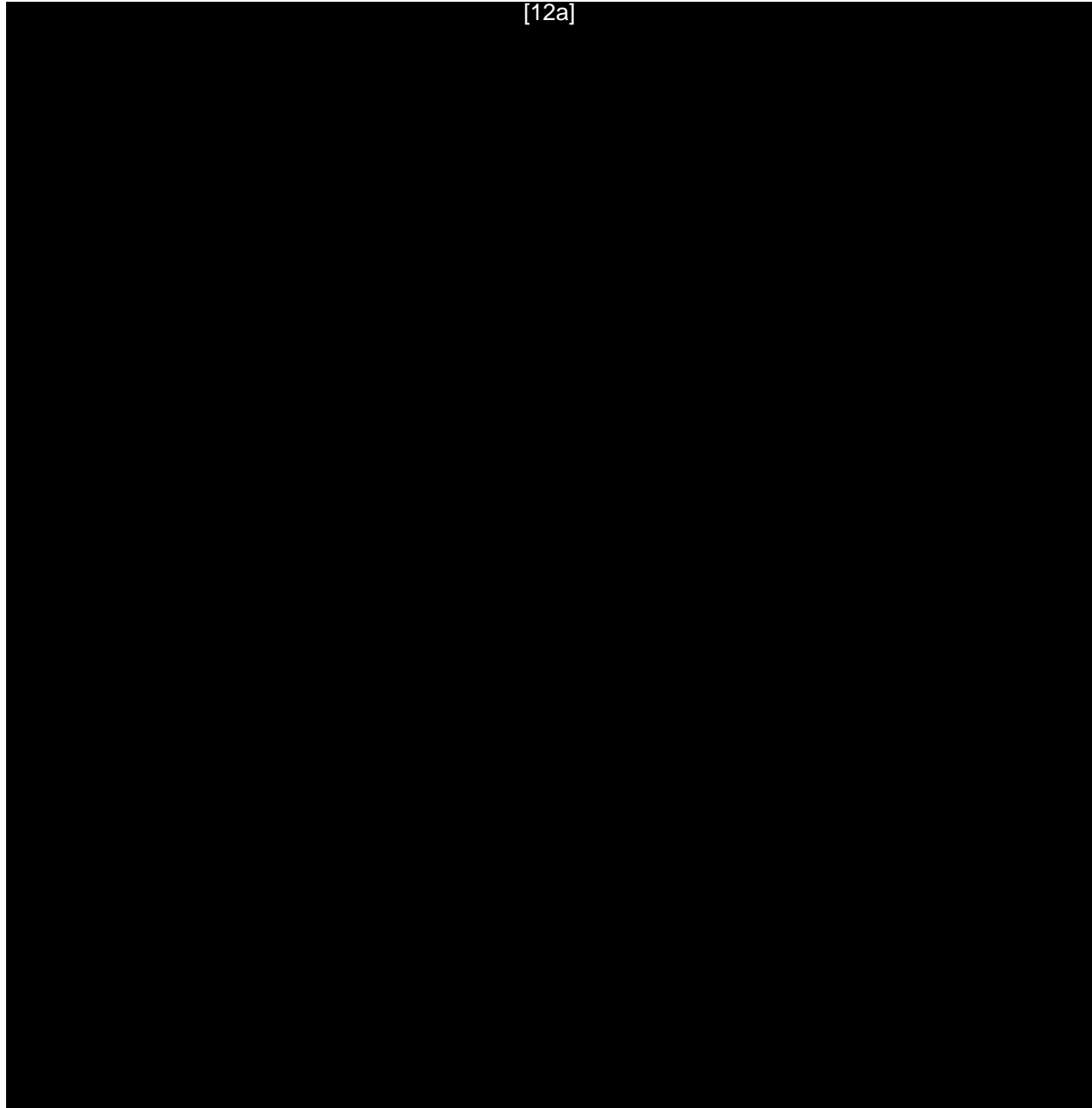


Exhibit 120. Call Origination via BCF – Location Routed



6.7. Call Transfer from an LPGCAMA PSAP

[12a]



Exhibit 121. Call Transfer from an LPGCAMA PSAP



6.8. Call Transfer from an LPGRFAI PSAP

[12a]

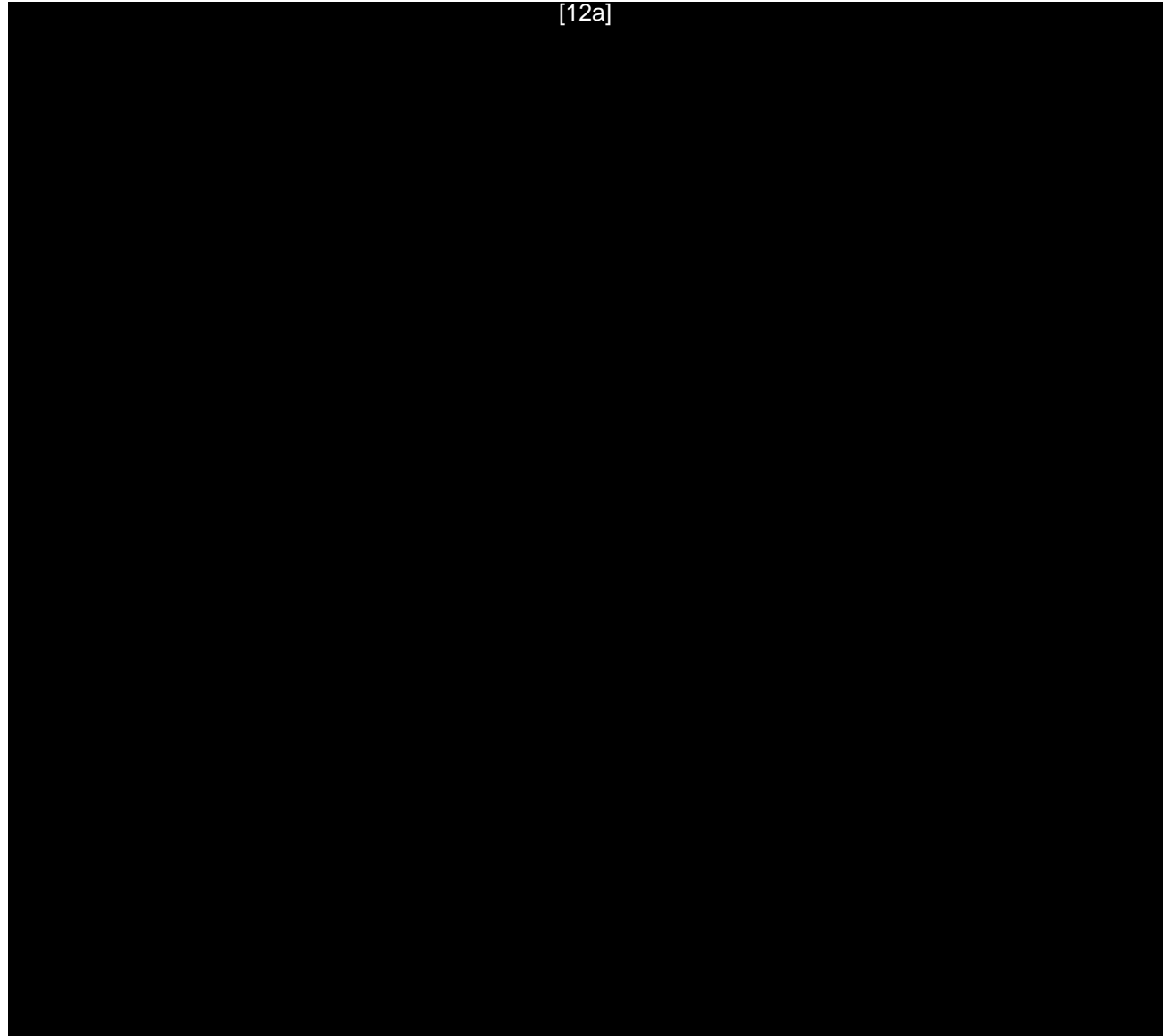


Exhibit 122. Call Transfer from an LPGRFAI PSAP



6.9. Call Transfer from an i3 PSAP

[12a]

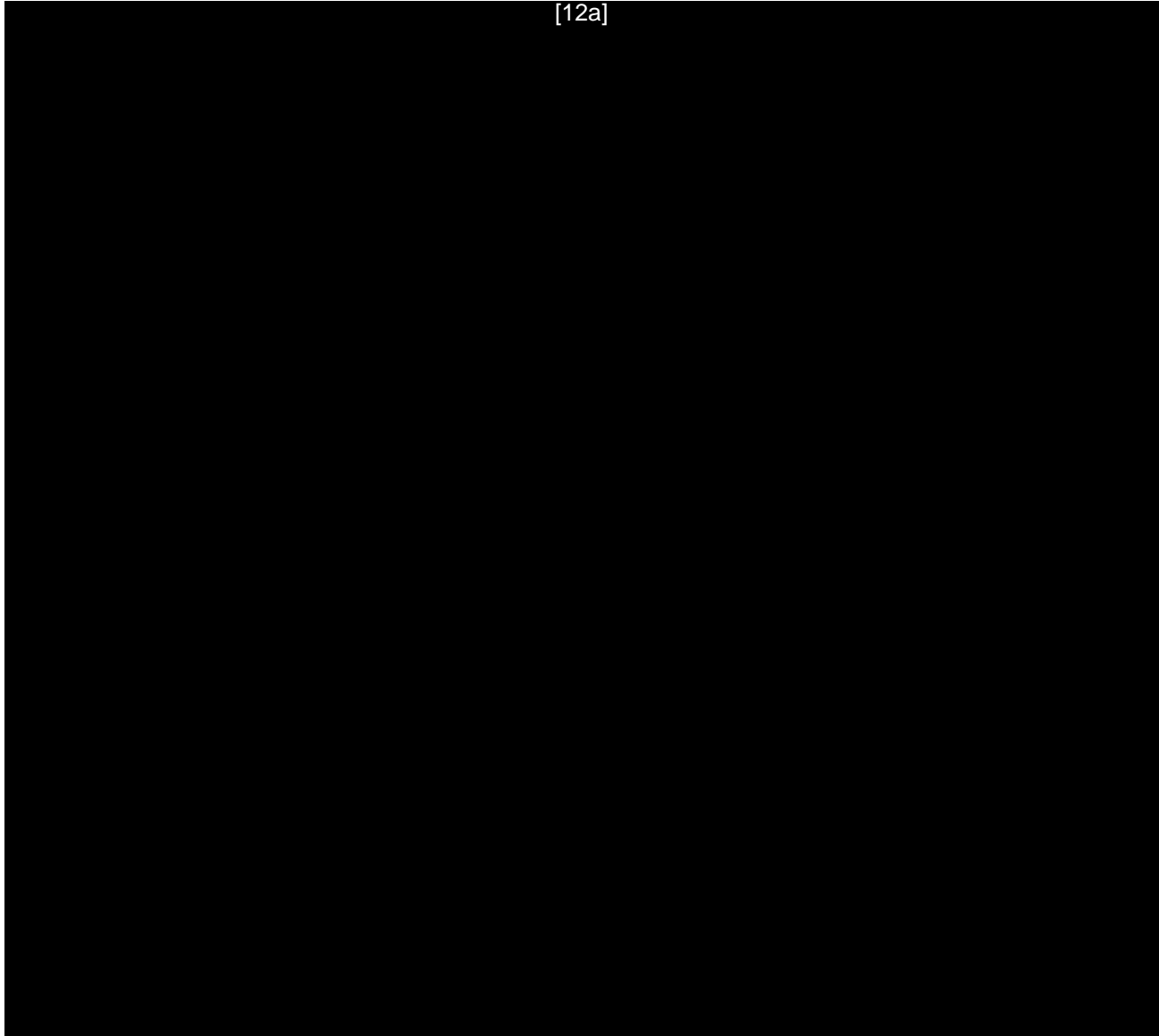


Exhibit 123. Call Transfer from an i3 PSAP



6.10. Call Transfer – “Figure 4 Reference” General Conferencing

[12a]

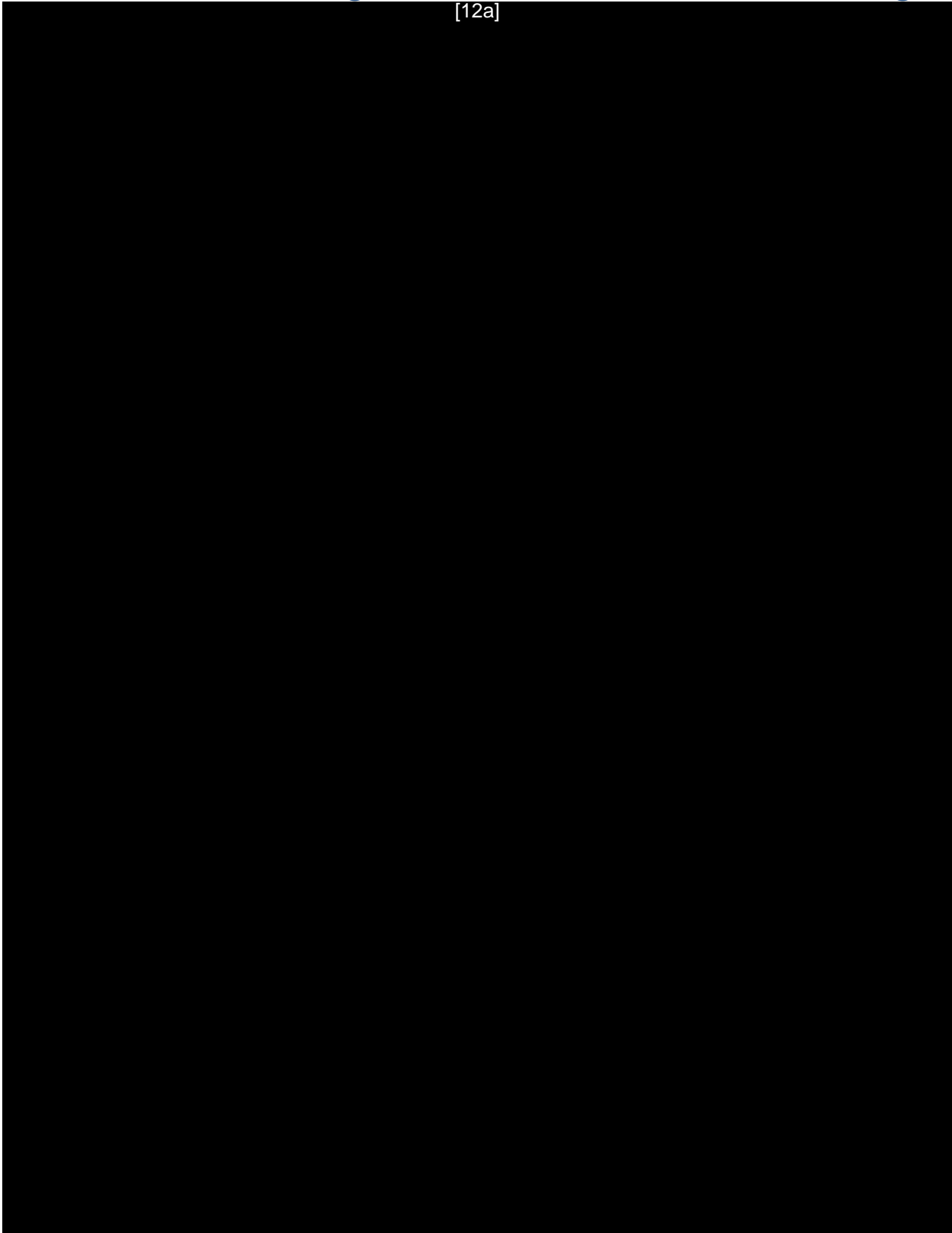




Exhibit 124. Call Transfer – “Figure 4 Reference” General Conferencing

7. MIL ESInet Requirements

11.1. Global ESInet Requirements [RFP 6.1]

As full “i3 compliance” is dependent upon functionality and features that reside outside of the ESInet itself (e.g., the LIS, external ECRF, etc.) or not yet fully defined, MIL is requiring an ESInet that is only based upon the i3 specifications as they pertain to an ESInet. Enhancements and allowances (e.g., optionally locating the LIF function within the ESRP), as identified in the following requirements are intended to 1) serve as placeholders where applicable (e.g., when the LIS function is fully deployed in the Originating Network, the NLIS function specified may be eliminated), or 2) provide additional functionality not specified, or not completely specified, in the NENA i3 architecture.

MIL is NOT dictating a specific implementation and/or architecture. That is, while the NENA standards specify various functional elements and/or network elements, nothing within this section shall be construed to mean each Functional Object needs to be implemented within a separate network element or that the BIDDER must preserve the NENA nomenclature for those Objects/Network Elements.

Finally, MIL’s intent is not to completely replicate the identified NENA documentation/requirements, rather the intent is to identify MIL’s mandatory requirements (unless identified otherwise) within the NENA referenced documents. NENA requirements not explicitly identified here are still deemed important, but non-compliance will not result in disqualification. Further, MIL understands that some of the functionality specified within this RFP is outside the scope of the NENA standards and may not be immediately available at the time of BIDDER’s response. In these instances, if any, the BIDDER must provide a timeline of availability for each such function and explicit indication that the function(s) will be implemented when it becomes available at no additional cost to MIL.

BIDDERS are encouraged to provide information regarding improvements or alternatives to these requirements in their responses.

We agree with the assessment that the ESInet and its functional elements are still evolving toward an i3 end-state. Where the i3 specifications allow or require interpretation, we have done so with the intent of adhering to the nature of the standard as much as possible. Therefore, while some aspects of our system may differ slightly from others who also follow the standard (e.g., the location of the Location Interworking Function [LIF] may vary as noted above), we strive to implement our solutions with a consistent interpretation of the specifications. Where functionality is not yet fully identified by NENA or other working groups, we have described our implementation as it is deployed today. Applicable future functionality will be available in our solution following ratification by the industry, and as long as that functionality is contained within the i3 specifications it will be implemented without additional cost to the Agency.

11.1.1. Federal Communications Commission (FCC) Rules – [RFP 6.1.1]

All equipment must conform to FCC Rules Part 15, Class A (commercial, non-residential radiation and conduction limits) for electromagnetic interference (EMI).

Our proposed solution uses commercial off-the-shelf (COTS) equipment that complies with all appropriate FCC, Underwriters Laboratories (UL)/Canadian Standards Association (CSA), Conformité Européene (CE), and NENA standards as they apply to such elements as electrical safety and electromagnetic interference for computer and telecommunications equipment.

11.1.2. Industry Standards – [RFP 6.1.2]

Where applicable, all equipment must comply with relevant industry standards, such as:

- Underwriters Laboratories (UL)



- *International Organization of Standards (ISO)*
- *Open System Interconnection (OSI)*
- *Institute of Electrical and Electronics Engineers (IEEE)*
- *National Emergency Number Association (NENA)*
- *American National Standards Institute (ANSI)*
- *Electronic Industries Alliance (EIA)*
- *Telecommunications Industry Association (TIA), (including ANSI/EIA/TIA-568 Commercial Building Telecommunications Wiring Standards), etc.*
- *Internet Engineering Task Force (IETF)*

The proposed [12a] solution is fully IP based and follows the Open Systems Interconnection (OSI) model. Furthermore, it does not require proprietary technology in order to use Layers 1–3, which are physical, data link, and network. All hardware contained in the [12a] solution meets or exceeds the latest applicable standards of the FCC, Electronic Industries Alliance (EIA), Telecommunications Industry Association (TIA), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), International Organization of Standards (ISO), and NENA at the time this RFP response was provided.

[12a] employs no proprietary standards or protocols, nor does it rely on open-source software products for call control. All products are 100 percent TCS engineered, built on open standards, and developed to meet NENA's published i3 standards. TCS developed its NG9-1-1 solution from the ground up to comply with NENA standards – including i3 – because they provide the best path for deploying a system that can leverage current technology while enabling customers to maintain an optimal system.

Our program management methodology incorporates best practices from ISO 9000 and more than 25 years of experience working with DoD, state and local governments, and commercial customers.

The solution complies with many existing NG9-1-1 and supporting standards from SDOs, including the following NG9-1-1 related standards development groups:

- Network Reliability and Interoperability Council Focus Group 7 subgroup 1A and 1B
- IETF, Emergency Context Resolution with Internet Technologies (ECRIT), Geopriv, and Phone Business Continuity Planning (BCP) working efforts
- Third Generation Partnership Project 2 (3GPP2) (et al.) IP Multimedia Subsystem (IMS) working group
- ATIS ESIF Task Force 34, et al.
- Joint ATIS/TIA WTSC-JSMS911 Native SMS text-to-9-1-1 Standard Specification

The current system supports, at a minimum, the following protocols:

- [12a]

The following audio CODECs:



- [12a]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

And the following applicable IETF requests for comment (RFCs):

- [12a]
- [Redacted]
- [Redacted]
- [Redacted]

The following NENA standards are used and/or adhered to:

- [12a]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Other standards/documents that are applied as relevant:

- [12a]
- [Redacted]

We are regular contributors to various standards groups and will maintain compliance with published standards as they are released throughout the length of this contract.

Our proposed solution uses commercial off-the-shelf (COTS) equipment that complies with all appropriate FCC, Underwriters Laboratories (UL)/Canadian Standards Association (CSA), Conformité Européene (CE), and NENA standards as they apply to such elements as electrical safety and electromagnetic interference for computer and telecommunications equipment.

11.1.3. Support for IPv4 and IPv6 – [RFP 6.1.3]

The ESInet shall support both IPv4 and IPv6. MIL will give priority to implementations which utilize a dual-stack approach. However, implementations which utilize tunneling will not necessarily be penalized if the BIDDER can show how security issues associated with tunneling can be solved or not come to bear.

Due to the nature and the number of disparate software and hardware components in an ESInet, the most efficient and effective IP routing solution requires a network that simultaneously supports IP version 4 (IPv4) and IP version 6 (IPv6) in its addressing and routing (that is, a



“dual-stack” approach). To that end, the proposed TCS solution includes software services and network components that can be configured to support both IPv4 and IPv6.

TCS software services [12a] are designed and certified to be configured for IPv6 address-based routing, messaging (including SIP), and media streams (i.e., Real-Time Transfer Protocol [RTP] for telephony and multimedia traffic). Where available, the TCS solution uses hardware components certified to simultaneously support IPv4 and IPv6 addresses for routing and networks. This combined IPv4/IPv6 platform is managed as call flow and routing designs are created, configured, and tested to ensure that potential errors are avoided. The TCS solution will be system engineered and certified to operate in an IPv6 environment during calendar year 2016.

TCS will work with Washington to engineer specific call flows, external network interfaces, and network routing to ensure that the required IP addressing schemes are operational.

11.1.4. IP Compliance – [RFP 6.1.4]

All SIP implementations shall comply with all SIP Methods, messaging and procedures as identified within “Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3”, NENA 08-003. All areas of non-compliance must be clearly identified in the BIDDER’s response. While non-compliance will not automatically disqualify any BIDDER, the nature of the non-compliance may adversely affect the BIDDER’s score. Any aspect of the BIDDER’s SIP implementation that is considered “proprietary” must be identified and will be disclosed to all potential PSAP CPE vendors to insure interoperability with the ESInet. BIDDERS not willing to disclose this information will be disqualified as not meeting a mandatory requirement.

[12a] is a software-based service that provides all the functionality required of ESInet-related functional elements as stipulated within NENA 08-003. Our SIP implementation is not proprietary.

11.1.5. SIP Interface Specification – [RFP 6.1.5]

While i3 CPE vendors have in principle all developed their implementations from the same NENA documents, this does not preclude the possibility of interworking problems when two (or more) different vendor implementations attempt to initially communicate.

Accordingly, BIDDER shall develop a SIP interworking specification which identifies all aspects of the Methods, messaging and procedures for any CPE vendor to successfully interwork with the Washington State ESInet. This specification must be made available to all potential CPE vendors at least six (6) months in advance of the initial turn-up of the ESInet.

TCS will develop a SIP interworking specification for any CPE vendor to successfully interwork with the Washington State ESInet and will make this specification available at least six months in advance of initial turn-up.

11.1.6. Existing SIP Compatibility – [RFP 6.1.6]

BIDDER shall provide a list of all i3 CPE vendors for which they have either:

- 1) *Already successfully interconnected, or*
- 2) *Have at least gone through “lab to lab” testing.*

TCS has accomplished interoperability testing (IOT) with not only own solution IP-based call-handling solution, but also with most notable vendors including Airbus, Emergency CallWorks/Motorola, NextGen (NGGT), Solacom, Intrado, Zetron, and Moducom. At the time of this writing, Emergitech and Tri-Tech are undergoing IOT as well.



11.1.7. Bandwidth per Audio Session (Call) – [RFP 6.1.7]

BIDDER shall provide a detailed accounting of the bandwidth required to transport each 9-1-1 voice call across the ESInet. Accounting is to include not only the RTP packet size and rate, but also the overhead attributable to each layer of encapsulation, including control (e.g., RTCP) and security encapsulations (IPsec, TLS, etc.). BIDDER need only supply this for the G.711 CODEC.

The Wide Area Network (WAN) will be configured to provide a [12a]

[12a] It is necessary [12a] to ensure utmost reliability and accurate voice retransmission.

11.1.8. Call Quality – [RFP 6.1.8]

While most (if not all) wireline calls will arrive via TDM with G.711 as the encoding and this equates to a maximum Mean Opinion Score (MOS) of 4.1, some wireless and VoIP calls for which other CODECs were utilized (e.g., G.729 with an attendant MOS (max) of 3.92) will likely be encountered as well.

Regardless of the CODEC employed for the call, the ESInet shall not degrade the received MOS by more than 0.5. To verify that the MOS is maintained, the BIDDER shall deploy the capability to automatically measure and record the MOS for each call and at both ingress and egress demarcation points in the ESInet.

While it is possible that, to a human listener, an undetectable decrease in the Mean Opinion Score (MOS) can occur due to transcoding between CODECs, we have engineered our systems to provide the best MOS possible. We use the ITU G.107 method of determining MOS through network-based appliances. Each call is automatically evaluated as the call is made, and similarly upon the telecommunicator's response, in order to capture voice quality. Other methods of determining MOS involve test dialing, whereas G.107 measures production voice transmissions. Using this method allows us to measure and record the call quality as it pertains to both ingress and egress to/from our network.

11.1.9. Guaranteed Bandwidth (Hard QoS) – [RFP 6.1.9]

Although NENA 08-003, Section 3.6 specifies the use of DiffServ (RFC2475) to manage 9-1-1 and 9-1-1-related traffic, MIL desires guaranteed bandwidth for all 9-1-1 traffic.

BIDDER shall identify the incremental cost, if any, of guaranteed Bandwidth over a DiffServ implementation in their response.

11.1.10. Time Changes – [RFP 6.1.10]

All systems that are associated with the ESInet and GIS/ALI database processes shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind will occur as a result of a date/time change up to thirty (30) years subsequent to the manufacture of the systems components. This shall include all application software, including any imbedded applications, and firmware as applicable.

We have engineered our systems to ensure no detrimental effects result from time changes.

11.1.11. No Single Point of Failure – [RFP 6.1.11]

With the exception of the End Offices connecting 9-1-1 callers to the Originating Network and the PSAPs themselves, no single point of failure will be allowed within the state of Washington NG9-1-1 System including any equipment and/or networking that may be located outside of the state, but involved in the provision of NG9-1-1 service. Any response which contains a single point, or multiple single points (i.e., within a series process) of failure will be disqualified. However, this does not include those PSAPs for which true physical diversity (for ESInet connectivity) is either unavailable or cost-prohibitive to provide.



The proposed solution is a NENA i3-compliant platform committed to the “five nines” standard (99.999 percent reliability) for providing the delivery and receipt of 9-1-1 calls. The proposed solution minimizes single points of failure; it is composed of redundant central system components that provide load sharing and load balancing with failover capability.

[12a]

We have designed [12a] to limit the possibility of downtime, both scheduled and nonscheduled. While it is possible that certain components of the system periodically could be interrupted, the redundant design of the system and its major components will minimize the impact of any downtime, and the failure of any particular component of the system should not be considered downtime [12a]

In general terms, the proposed [12a] solution has been engineered end-to-end to achieve the greatest degree of high availability at every level. All components of the system are continuously exercised, so when there is a failure of a component it is not the first time that component has been used. The overall peer-to-peer (P2P) architecture allows any component to be removed while the remaining peers pick up the processing demands of the failed component. In addition to the P2P architecture, TCS uses load-balancing schemes to distribute the load evenly over the components.

The first layer of diverse and redundant connectivity begins with the network carrier. The TCS ESInet routing architecture rides on top of that, embodied by the installation of redundant hardware at [12a] sites, and with all elements available on a real-time basis throughout the life of the system. This means there will be no functional single point of failure anywhere along the ESInet with regard to the delivery and receipt of 9-1-1 calls. This geographic diversity permits the system to operate as a single entity, even under the most catastrophic of conditions, and its design provides for a seamless transition in call-processing capacity from platform to platform and site to site.

11.1.12. “365 X 24 X 7” ESInet Monitoring System – [RFP 6.1.12]

All facets of the ESInet system shall be monitored on a staffed (i.e., humans always present and on-duty at the monitoring location) 365 X 24 X 7 basis.

The Monitoring system shall also maintain logs of all ESInet alarms and notifications regardless of severity level. The Monitoring System logs shall also record any loss of capability to monitor the ESInet, either in whole or part and reflect the time the capability was lost or impaired and the time at which the capability was fully restored. See Section 6.2.21 for detailed logging requirements.

Monitoring is provided by the TCS [12a] (see Exhibit 125), with a fully staffed 24x7 facility in [12a] data center and an equally capable [12a] backup facility [12a]. The TCS [12a] is ISO 27001 and ISO 9001 certified. It provides continuous, subscription-based service designed to deliver real-time protection to the system. The TCS [12a] will:

- Detect problems quickly
- Notify stakeholders
- Respond appropriately
- Restore critical services
- Provide root-cause analysis (RCA) for Service Impairment Level (SIL) 1 and SIL 2 events (high impact to service)
- Provide 24x7 monitoring and operations support
- Make full use of georedundant advanced network monitoring and reporting tools (e.g., HP OpenView, Remydy) optimized by full-suite vendor support and TCS trained engineers
- Leverage experienced monitoring and engineering staff



Exhibit 125. TCS Network Operations Center

The services available with TCS [12a] monitoring include:

- | | |
|------------------------------------|--|
| • Availability monitoring | • Incident response |
| • Event handling | • Policy-based incident handling, based on SLA |
| • Event monitoring | • Packet analysis |
| • Event correlation | • Respond/restore/remediate |
| • Event escalation | • Feed and receive incident alerts |
| • Co-location of critical services | • Monthly incident reporting based on SLA requirements |
| • Disaster recovery | |
| • Post-event analysis | |

The details of network events, including the loss of monitoring capability, are recorded in the event files. Analysis of these events allows our staff to correlate a large variety of events,



including the loss of monitoring capability. Alarms and notifications are logged, regardless of severity level.

11.1.13. Automatic Fail-Over – [RFP 6.1.13]

Any redundancy mechanisms that employ “fail-over” procedures must be 100% automatic and not require human intervention. Further, once a fail-over procedure is invoked, a Major alarm will be raised and maintenance personnel shall immediately become engaged to determine: 1) why the procedures were invoked, and 2) that the fail-over elements are operating correctly.

Finally, MIL requires that any fail-over or redundancy mechanisms will be periodically tested to insure they function as designed. BIDDERS shall describe in detail all procedures and/or functionality used to insure proper operation of fail-over/redundancy measures.

[12a] is modular in design, using COTS components that support the current and future needs of the PSAP. We engineered [12a] ESInet to meet or exceed 99.999 percent reliability. Our solution consists of redundant next generation core services and IP network components that provide load sharing and load balancing with full failover capability. [12

[REDACTED]

The overall distributed component architecture allows any component to be removed while its remaining peers pick up the processing demands of the removed component. In addition to the distributed computing architecture, we use load-balancing schemes to distribute the load evenly over the components. This provides the highest level of availability and differentiates our solution from others on the market. No levels of service are compromised due to the failure of a single module or component, and all components in the system are regularly exercised and therefore known to be operational. Any failures in the system are appropriately alarmed, logged, and escalated through our [12a] for resolution.

Due to the [12a] design, the system is continually exercised to ensure proper operation. During maintenance events, traffic may be swung to one side of the redundant system to avoid any potential issues with the maintenance itself. [12a]

11.1.14. Shared Infrastructure – [RFP 6.1.14]

MIL understands that potential BIDDERS may utilize infrastructure that is “shared” (i.e., VPNs on an MPLS network) between other customers in addition to MIL. In no case shall any failure, administrative action, or any other activity not related to the Washington ESInet for or on behalf of other customers impact the Washington ESInet. BIDDER shall provide a detailed description on how this will be achieved.

[REDACTED]

Our standard and proven approach to a shared environment is to partition our gateways and to control application resources through data segregation. This is the same approach and structure we use in our Mobile/VoIP Positioning Center (MPC/VPC) call-routing applications, where we



process more than 200,000 calls each day. Optionally and at additional expense, we can provide a dedicated solution, wherein all hardware would be solely for the use of the state. We have designed and priced the standard approach in order to provide the most cost-effective solution, but we are happy to discuss all alternatives with the Agency to arrive at a final design, as noted in the Executive Summary.

For the standard approach, we have had very good success in managing our customer's availability through the use of software controls and a very detailed change management plan. Our change management process is known as an Installation and Backout Plan (IBOP). Depending on the complexity of the change, TCS uses either an express IBOP or a full IBOP. For the most complex changes, TCS engineers complete a full IBOP, which typically is written over a several-week period and includes multiple meetings in which engineers discuss the best design, review services impacted, and determine the most efficient steps for implementation and backout in case such action becomes necessary. Before implementing an IBOP, TCS Project Management coordinates a final technical review and a final management review. Representatives of the state and affected stakeholders are encouraged to participate in both meetings.



Exhibit 126 below is a sample screenshot of an express IBOP.

Expressibop

Operations Engineering Change Control Submission Form

Hello: tooulombe

Group: **Network Engineering** Type: **General**

Lead Integrator: tooulombe Express OECC Number assigned automatically.

Purpose: Update BGP configuration to allow Monitoring Network to Santa Clara

General Overview: Request by customer to Allow Santa Clara network to be monitoring
 500Max: 0

Expected Impact: BGP routes will be updated

Possible Worse Case Impact: BGP routes could go bad; restart BGP process [Clear ip bgp soft]

Impacted Devices: seawm-voip-rtl

Change Steps: 1975Max: 0
 conf t
 router bgp 63212
 neighbor 7.49.29.127 remote-as 67323
 neighbor 7.49.29.127 route-map monitoring out

Verify Steps: sho ip bgp route
 sho ip bgp neigh 7.49.29.127

Individuals Included:
 SE: _____
 NOC: _____
 Tools: _____
 QA: _____

E-Mail Notification list: (Choose which groups to notify.) NE & NocMonitoring are default notifications.
 UNIXStaff/SEs Integration Engineering

** Enter other alias names to notify. (use a Semicolon (;) to separate the names). (@Telecomsys.com not required) **

IBop Start Date: 11/17/2010 Hr: 17:5T 49 Reset

IBop Completion Date: 11/17/2010 Hr: 18:5T 49 Reset

Click if Conference Bridge required.


Send For Manager and Peer Approval Only

Submit Reset [ExpressOECC Home](#) [ExOECC Info](#)

Exhibit 126. Express IBOP Screenshot



Exhibit 128 below is a blank IBOP template that shows the type of information captured.



TCS TeleCommunication Systems
Enabling Convergent Technologies®

**IBOP
IMPLEMENTATION AND BACK-OUT PLAN**

MAINTENANCE WINDOW SUMMARY

IBOP Name	Enter the name of the IBOP
Purpose	Why is this being done
Date	MM / DD / YYYY
Time	HH:MM -- HH:MM Pacific Time
Services/Equipment	What services are going to be affected?
Description	Summarize what is being done for internal audience consumption. <i>i.e., the suck-a server is hosed and needs to be rebooted.</i>
External Description	Summarize what is being done for external audience consumption. <i>i.e., TCS is performing server maintenance.</i>
Impact	What will happen as a result of the change? or What could happen if things go wrong?
Notification	External (name specific customers/carriers as necessary) and Internal
Notification Timing	?? Hours <small>(see NOC Boilerplate on KMS for guidance)</small>
Release Contains	You may optionally include details about the release here (e.g., a bulleted list).

xxx xxx xxx pin xxx

xxx xxx xxx pin xxx

N/A
No NOC bridge needed

Tested in PPE?
Date: mm/dd/yyyy

Test Comments: (especially if no testing occurred)


IMPLEMENTATION TEAM

Title	Name	Reviewed by	Date
Lead Integrator			
ATAC			
NOC		Not required	
SE			
NE			
Carrier Software			
CTSO		Not required	
Provisioning		Not required	
Project Manager		Not required	
Development		Not required	
Deployment		Not required	
NSS		Not required	

Exhibit 128. Blank IBOP Template



Exhibit 129 below illustrates a blank IBOP template for the pre-implementation NOC information.



TCS TeleCommunication Systems
Enabling Convergent Technologies®

IBOP
IMPLEMENTATION AND BACK-OUT PLAN

PRE-IMPLEMENTATION NOC

#	Task Description	Comments
<input type="checkbox"/>	1. NOC – Determine what carriers require notification. a) Notify carriers at least 24 hour in advance of the maintenance window. b) Please follow TCS notification guidelines not included in this document.	
<input type="checkbox"/>	2. NOC – Log carrier’s contact, include time, type of contact (email, vmail, etc). Include all pertinent information.	
<input type="checkbox"/>	3. NOC – Email Integration Team (including Ops PM) confirming carrier notification.	
<input type="checkbox"/>	4. NOC - E-Mail TCS Internal Conference Bridge number to Ops & Dev staff by Xpm, XX/XX/2007.	
<input type="checkbox"/>	5. NOC – Set up internal conference bridges at X:XXpm.	
<input type="checkbox"/>	6. NOC – Monitor for associated alarms during maintenance window.	
<input type="checkbox"/>	7. NOC – Verify good traffic flow by looking at normal system message flow.	
<input type="checkbox"/>	8. NOC – Prepare to take notes during maintenance window	
<input type="checkbox"/>	9. Lead Integrator – Determine necessary changes to current Backup NOC and Disaster Recovery processes and procedures and make required updates as needed. This may include: a) NOC Tools: implementation of new, decommissioning of old, and/or modification of existing tools – documentation updates may be required b) Active/Standby platforms: temporary or permanent modifications to applications, hardware, and/or connectivity which would affect existing or require new failover procedures in the event of a disaster c) Telephone systems: upgrades and/or maintenance of Seattle PBX, Phoenix virtual PBX, PRI voice trunks, and/or SIP software phone services and/or accessibility which would affect Backup NOC voice services	
<input type="checkbox"/>	10. NOC – (Add specific tasks here)	

OE (IF REQUIRED)

#	Task Description	Comments
<input type="checkbox"/>	11. OE (XXX)- (Add specific tasks here)	
<input type="checkbox"/>	12. DBA (XXX) – (Add specific tasks here)	
<input type="checkbox"/>	13. NE (XXX) – (Add specific tasks here)	

GIS (IF REQUIRED)

#	Task Description	Comments
<input type="checkbox"/>		

Exhibit 129. Blank IBOP Template for Pre-implementation NOC Information



Exhibit 130 below illustrates a blank IBOP template for the implementation information.


		IBOP IMPLEMENTATION AND BACK-OUT PLAN
<input type="checkbox"/>	14. GIS (XXX) – (Add specific tasks here)	
SBSD (IF REQUIRED) # Task Description Comments		
<input type="checkbox"/>	15. SBSD (XXX) – (Add specific tasks here)	
X:XXPM TO X:XXPM - IMPLEMENTATION # Task Description Comments		
<input type="checkbox"/>	16. ??? (XXX) – Request a TCS system health check by NOC.	
<input type="checkbox"/>	17.	
<input type="checkbox"/>	18.	
<input type="checkbox"/>	19.	
<input type="checkbox"/>	20.	
<input type="checkbox"/>	21.	
X:XXPM TO X:XXPM - POST IMPLEMENTATION – VALIDATION # Task Description Comments		
<input type="checkbox"/>	22. Lead Integrator (XXX) – Confirm that the functionality (restored or new) provided by the kit or patch is running as expected. by NOC.	
<input type="checkbox"/>	23. ??? (XXX) – (Add specific tasks here)	
<input type="checkbox"/>	24. Lead Integrator or PM (decided during IBOP review) – Send out successful/unsuccessful email notification to team. Include #TCS_NOC in email list.	
<input type="checkbox"/>	25. NOC - Send out external and/or internal maintenance window completion notification with final disposition.	
<input type="checkbox"/>	26. NOC - Forward notes or log to the following distribution list in Outlook: "MWnotes" and store notes in PM folder.	
BACK-OUT PLAN # Task Description Comments		
<input type="checkbox"/>	27. NOC – Send out external and/or internal maintenance window completion notification with final disposition.	
<input type="checkbox"/>	28. LI– Send out detailed email summarizing Maintenance Window and reasons for back-out.	
<input type="checkbox"/>	29. NOC - Forward notes or log to the following distribution list in Outlook: "MWnotes" and store notes in PM folder.	
DISASTER RECOVERY # Task Description Comments		
<input type="checkbox"/>	30. Document any changes to Disaster Recovery plans currently in place that will need to be updated as a result of this IBOP. This includes changes to documentation, procedure, or policy as noted	

Exhibit 130. Blank IBOP Template for Implementation Information



Exhibit 131 below illustrates a blank IBOP template for the approval signatures.

[12a]



Exhibit 131. Blank IBOP Template for Approval Signatures

Evaluation

As mentioned earlier, all change requests and project evaluations receive careful consideration to factor in all aspects of change, including authorization, clarity, compliance, feasibility, identification, procedure, recovery, resources, security, side effects, test plan verification, and cost. The TCS client service manager, [12a], leads review discussions and invites all potentially impacted parties to arrive at a comprehensively documented scope of change. The TCS client service manager presents and delivers the final scope of change to the approving authority for approval or rejection. The TCS client service manager also documents and tracks reasons for approval or rejection.

Implementation

Upon approval from Agency governance or the appointed designee, TCS plans the change. For greater efficiency and accountability for large changes, the TCS client service manager identifies appropriate entities and involves their coordination in every critical step of implementation. The TCS client service manager performs duties identified in the Scope of Services, including logging entries to record the actual work performed, the time and date of the work, and the



results of the test plan. If unexpected problems arise, the recovery procedure is invoked and documented, and the change is returned for additional review.

Completion

TCS updates all documents and records in the management system as required by the change and publishes the actual steps taken so this information is available to the Agency.

In accordance with Project Management Institute (PMI)-recognized best practices, the TCS PMO documents lessons learned and a project performance summary at the close of every project. TCS maintains a database of lessons learned, which is available to all resources within the organization to query for future projects. In addition, all project-specific documents and related material are stored in a secure/backup shared location for archive and audit purposes after project closure.

Through years of refinement, our IBOP process has become a very valuable change management tool. We have full confidence that our designs and processes will protect the state's interests in our shared environment.

11.1.15. Outage Notification – [RFP 6.1.15]

Any ESInet outage that results in the inability of the ESInet to deliver a 9-1-1 call to a single PSAP, multiple PSAPs or all PSAPs shall be reported immediately, but no more than within 15 minutes of outage, to MIL, the affected County 911 Coordinators and PSAP(s) upon detection. Attachment G will be updated to include contact information for sending said notification(s) to the affected PSAPs and provided to the Successful BIDDER.

Notifications should first be via a phone call and followed-up with an email (regardless of whether the call was answered or not) to the affected PSAPs, AND MIL must be notified by sending an email to E911outages@mil.wa.gov or by calling 1-800-258-5990 should access to email be unavailable.

TCS has a robust notification process that accommodates the Agency's need. On outages that result in the inability to deliver calls, an alarm condition will be raised and NOC troubleshooting will begin immediately, and the notification processes [12a]. The TCS [12a] technical support tiers and responsibilities are:

- Tier 1: NOC
 - Incident detection and management
 - Incident triage and troubleshooting
 - Resolution or escalation of issues that cannot be resolved in a timely manner
- Tier 2: Advanced Technical Assistance Center (ATAC)
 - 24x7 application subject matter experts (SMEs)
 - In-depth troubleshooting and analysis
 - Resolution of call-quality errors
- Tier 3: Operations Engineering
 - 24x7 network engineers/system engineers
 - Tier 4: Software engineering
 - 24x7 software development



As shown in Exhibit 132, TCS sends at least three color-coded notifications for each NOC event.

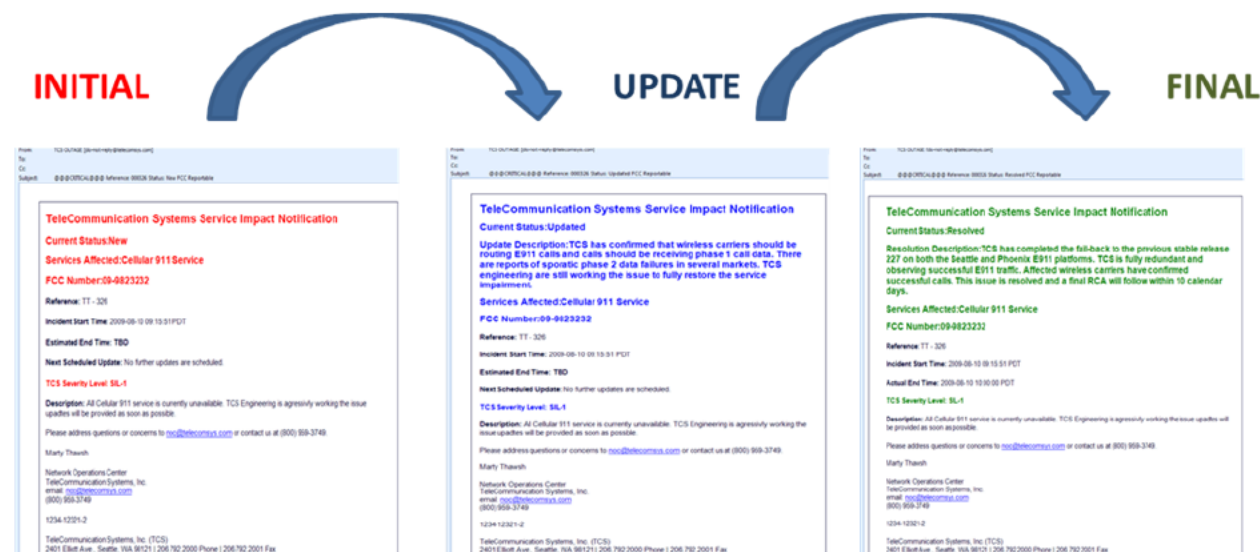


Exhibit 132. NOC Event Notification Process

The final NOC notification report will contain a summary of the event to serve as the incident report. A formal RCA will follow within 10 days.

Events that require notifications will first be via a phone call and then followed-up with an email to the PSAPs, and the Agency will be notified by sending an [12a] [redacted] should access to email be unavailable.

11.1.16. Failed Calls Report – [RFP 6.1.16]

In the event of an outage and subsequent restoral of service, the BIDDER shall provide MIL will a list of all 9-1-1 calls that could not be delivered to a PSAP (i.e., failed calls) within fifteen (15) minutes of restoral. The list shall contain;

- County of call origination
- PSAP for call destination (if determinable)
- ANI/pANI
- Call Back (wireless/VoIP) Number (Optional)
- Carrier (from which the call originated)
- Start time of call MM/DD/YYYY, hh.mm.ss.s PTZ
- End time of call MM/DD/YYYY, hh.mm.ss.s PTZ

Lists shall be provided in a format that can be sorted based on;

- County
- PSAP
- Carrier

We will deliver a failed calls report within 15 minutes of an outage restoral, with the requested information contained in the report. The report can be sorted based on county, PSAP, and carrier.

11.1.17. Call Back Numbers for Failed Calls – [RFP 6.1.17]

MIL is highly interested in BIDDER providing a service wherein, the BIDDER would contact the appropriate Wireless/VoIP carrier to obtain the “call back number (CBN)” for the failed calls identified within 6.2.16 of this section.



That is, Wireless and (some) VoIP calls will typically contain only the pseudoANI (pANI) in the signaling used between the Originating Network and the ESInet (LNG/BCF). As such, each Wireless or VoIP provider must be contacted to obtain the telephone number (e.g., Mobile Directory Number (MDN)) to call back the person that attempted to place the 9-1-1 call. Collection of the CBN shall not delay the reporting required by 6.2.16, rather the report shall effectively be enhanced with the addition of the CBNs as they become available. It is understood 1) that BIDDER will only be capable of initiating the request to the respective Service Providers and will have little or no control over if and when a response is received and 2) also that MIL may need to become involved in the process to obtain CBNs.

TCS will provide a report for MIL that identifies the CBN of wireline, VoIP i2, and wireless calls for calls identified in the Failed Calls report. The CBNs related to p-ANIs will only be from the carriers supported by the TCS MPC/GMLC/VPC. For carriers not serviced by a TCS MPC/GMLC/VPC, TCS will make a reasonable effort to retrieve the CBN for failed calls from these carriers and/or their service providers. MIL may be required to provide a formal request/letter of authority to TCS (or otherwise authorize TCS in writing) to act on behalf of MIL in order to retrieve the CBN for call failures from carriers and/or their service providers.

11.1.18. Call Back Number System – [RFP 6.1.18]

As a complement to 6.2.16 and 6.2.17, BIDDERS are encouraged to propose an automated system wherein the BIDDER provides a Web Site that allows each County/PSAP and MIL (upon receipt of outage notification) to login (User Name and Password required) and obtain this information in real-time (as it comes in). Further upon login, only data relevant to the affected PSAP(s) provider will be displayed, with the exception of MIL which would be presented with all data generated from the failure. This would allow the PSAP operator to immediately begin working any wireline calls and address the Wireless and VoIP provide calls as the callback numbers are received from each Wireless/VoIP provider.

All displayed information should be easily exportable. This capability shall be in-service no later than Q3 2018.

TCS will provide a web portal for MIL that replaces the CBN report from Section 2.7.5 which identifies the CBN of wireline, VoIP i2 and wireless calls for calls identified in the Failed Calls report. The CBNs provided will only be from the carriers supported by the TCS MPC/GMLC/VPC. The CBNs related to p-ANIs will only be from the carriers supported by the TCS MPC/GMLC/VPC. For carriers not serviced by a TCS MPC/GMLC/VPC, TCS will make a reasonable effort to retrieve the CBN for failed calls from these carriers and/or their service providers. MIL may be required to provide a formal request/letter of authority to TCS (or otherwise authorize TCS in writing) to act on behalf of MIL in order to retrieve the CBN for call failures from carriers and/or their service providers. County 911 Authority – [RFP 6.1.19]

As MIL is procuring the ESInet service on behalf of the County 911 Authorities within the state, BIDDER must comply with:

- 1) Any decisions as to real-time (call) routing changes (e.g., default ESNs or PRF rules) that are communicated to BIDDER from the County 911 Authority.*
- 2) Additions or modifications to GIS/ALI data.*
- 3) Call disposition treatment. For example, return BUSY to wireless caller if all trunks designated as Wireless are occupied, but wireline trunks are available.*

TCS will comply with county 9-1-1 authorities with regard to real-time routing changes, additions or modifications, and call disposition treatment. GIS and ALI data will follow the data management processes as requested in this RFP, resulting in a [12a] implementation timeline. Call disposition rules are handled in our PRF, which can be updated through the use of a dashboard portal. Routing changes can be performed through data management processes or by creating on-the-fly (OTF) polygons in the dashboard portal.



The PRF associated with the ESRP not only provides the basic policy function as defined in NENA Standard 08-002 and 08-003 (PSAP state, congestion state, time of day), but also allows for dynamically created, OTF call-policy routing based upon geographic call origination, considered to be an enhanced policy routing function (E-PRF).

Response plans, which determine backup or alternate PSAPs that will answer 9-1-1 calls in the event of a major crisis, are used to dynamically and quickly change the PSAPs that will receive calls. Every region-to-PSAP association has a response plan setting to ensure that callers from particular regions will be routed to different PSAPs according to the rules that make up the active response plan.

Active response plans can be established over the web or within the solution’s administrative dashboard and configuration application.

Creating OTF routing polygons is accomplished via the GUI’s drawing tools. Exhibit 133. shows an example of the creation of a temporary routing polygon to facilitate responses during a power outage, the extent of which is outlined in green.

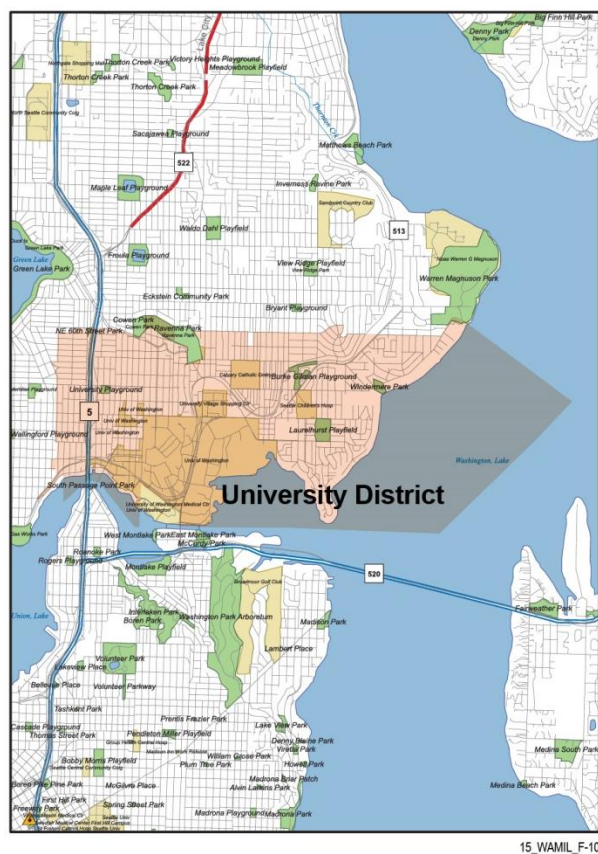


Exhibit 133. On-the-Fly Polygon Creation



11.1.19. Identification of Location of Critical Infra-Structure – [RFP 6.1.20]

BIDDERS shall identify the physical location of all points of concentration/aggregation of facilities and critical network functions/elements such as, but not limited to, LNGs, SBCs, ESRPs, ECRF, LIS, etc. MIL reserves the right to request alternative locations or mitigation measures, should any planned location(s) be deemed to have survivability issues.

We design our systems with complete redundancy. Critical infrastructure will exist in our data centers, [12a]

[12a] The data centers, which are known as CLCs, make up the majority of the [12a] solution. The CLCs will house the applications (e.g., ESRP/PRF; ECRF/LVF; SIF; logging and informational databases; security, monitoring, and portal applications), [12a]

[12a]
[12a]
[12a]
[12a]

11.1.20. Implementation Timeline(s) – [RFP 6.1.21]

BIDDERS shall provide a detailed implementation timeline for all aspects of their proposed solution.

Exhibit 134 shows a detailed Gantt chart of the [12a] ESInet implementation timeline.



[12a]



Exhibit 134 [12a] ESInet Implementation Schedule



11.1.21. Acceptance Test Plan (ATP) – [RFP 6.1.22]

MIL will require a written ATP as part of the final contract and will be developed as part of the Stage 5 proceedings. While Attachment H provides an example outline of MIL's minimum expectations as to what the ATP will encompass, BIDDER shall provide a preliminary ATP outline to serve as a starting point for development of the final ATP.

TCS will work with Washington in good faith to establish a reasonable plan and other details for system acceptance testing.

Below are representative excerpts from the CLC test plan and PSAP test plan.

TCS' CLC and PSAP test plans have been developed by TCS through expenditure of its own time, money and other resources. Such test plans also include information not necessarily known to TCS' business competitors and could be used by such business competitors to the competitive disadvantage of TCS. Accordingly, TCS believes that the details of TCS' test plans included in this response should be protected as financial, commercial, and/or proprietary information belonging to TCS exempt from public disclosure pursuant to the provisions of RCW 42.56.270, and should be redacted from any public records disclosure of the TCS proposal. In addition to and notwithstanding the status of such information as financial, commercial, and/or proprietary information belonging to TCS as described above, TCS also notes that the Agency may wish to consider limiting public disclosure of such portions of TCS' response based on general concerns for public security and safety and pursuant to the exemption of specialized details of security arrangements from public disclosure permitted pursuant to the provisions of RCW 42.56.420(4).

CLC Test Plan

Shown below are excerpts from the 155-page CLC test plan, including cover page, table of contents, introduction, select test cases, and test coverage summary. TCS has used test plans such as this in previous successful ESInet deployments.

The test plan excerpts shown below are proprietary.



TeleCommunication Systems Inc.
2401 Elliott Avenue
Seattle WA 98121
Phone 206 792-2000
Fax 206 792-2001
www.telecomsys.com




NG9-1-1_TCS CLC & ESInet Generic Test Plan

Test Cases for Call Logic Centers & All Interfaces on TCS/Customer NG9-1-1 Network

Document Number: TCSP-208

Document Release 1.0

December 2015

The xypoint location platform
from 



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

[12a]

A large, solid black rectangular redaction box covers the central portion of the page, obscuring all text and graphics that would otherwise be present.



[12a]





2.8. TCS NG9-1-1 Selective Routing And Location Applications	78
2.8.1, NG-911 Applications – LNG Service.....	79
2.8.2, NG-911 Applications – ESRP Service.....	81
2.8.3, NG-911 Applications – LPG (NIF and LIF) Service.....	82
2.8.4, NG-911 Applications – ECRF Service.....	84
2.8.5, NG-911 Applications – LIS Service.....	86
2.8.6, NG-911 Applications – LSRG Service.....	88
2.8.7, NG-911 Applications Failover – LNG Service.....	90
2.8.8, NG-911 Applications Failover – ESRP Service.....	92
2.8.9, NG-911 Applications Failover – ECRF Service.....	94
2.8.10, NG-911 Applications Failover – LIS Service.....	96
2.8.11, NG-911 Applications Failover – LPG (NIF and LIF) Service.....	98
2.8.12, NG-911 Applications Failover – LSRG Service.....	100
2.8.13, NG-911 Applications – Call Test.....	102
2.8.14, NG-911 Applications – Call Test.....	104
2.8.15, NG-911 Applications – Call Test.....	106
2.8.16, NG-911 Applications – Call Test.....	108
2.8.17, NG-911 Applications – Call Test.....	109
2.8.18, NG-911 Applications – Call Test.....	111
2.8.19, NG-911 Applications – Call Test.....	112
2.9. TCS Monitoring and Alarming Components in the NG9-1-1 Platform ...	113
2.9-1, Monitoring and Alarming Components in the NG9-1-1 Platform.....	113
2.9-2, Monitoring and Alarming Components in the NG9-1-1 Platform.....	114
2.9-3, Monitoring and Alarming Components in the NG9-1-1 Platform.....	115
2.9-4, Monitoring and Alarming Components in the NG9-1-1 Platform.....	116
2.9-5, Monitoring and Alarming Components in the NG9-1-1 Platform.....	117
2.9-6, Monitoring and Alarming Components in the NG9-1-1 Platform.....	118
2.9-7, Monitoring and Alarming Components in the NG9-1-1 Platform.....	119
2.9-9, Monitoring and Alarming Components in the NG9-1-1 Platform.....	119
2.9-10, Monitoring and Alarming Components in the NG9-1-1 Platform.....	121
2.9-11, Monitoring and Alarming Components in the NG9-1-1 Platform.....	122
2.9-12, Monitoring and Alarming Components in the NG9-1-1 Platform.....	123
2.9-13, Monitoring and Alarming Components in the NG9-1-1 Platform.....	124
2.9-14, Monitoring and Alarming Components in the NG9-1-1 Platform.....	125
2.9-15, Monitoring and Alarming Components in the NG9-1-1 Platform.....	126
2.10. ESINET Connection - MPLS to CLCs	126



2.10-1, ESINET Connection– MPLS to CLC - Circuit Connectivity (need to replace
 ESI router name with correct router name and other highlighted items)..... 127
 2.10-2, ESINET Connection– MPLS to CLC - Circuit Connectivity 130
 2.11. ESINET Connection - MPLS to PSAPs 132
 2.11-1, ESINET Connection– MPLS to PSAP - Circuit Connectivity 132
 2.11-2, ESINET Connection– MPLS to PSAP – 2 way Voice Testing 136
 2.12. PSAP Equipment – Pre cut-over to NG9-1-1 Network 138
 2.12-1, PSAP TCS Hardware Installation – ALI connectivity 1 138
 2.12-2, PSAP TCS Hardware Installation – ALI connectivity 2 (change NENA Server
 names to reflect correct network TCS is building) 139
 2.12-3, PSAP TCS Hardware Installation – ALI connectivity 3 140
 2.12-4, PSAP TCS ALI connectivity 4 142
3. Test Coverage Results Summary 144
4. Document Revision History 147

NG9-1-1 Customer

Test Cases for Call Logic Centers

1. Introduction

1.1. Purpose

This document provides TCS Next Generation 9-1-1 (NG9-1-1) Network Solution customers (“customer”) with an overview of the test cases that TCS will execute for each Interface and/or System Component on the NG9-1-1 System TCS is delivering for the customer. This document contains:

- a. Description of each Interface and/or System Component
- b. Testing Goal of each Interface and/or System Component
- c. How TCS will test each Interface and/or System Component
- d. Per each Interface and/or System Component:
 - a. Test cases
 - b. Expected results for each test case
 - c. How TCS will verify each Test Case

This test plan was developed to prove to our NG9-1-1 customer, that the NG9-1-1 Solution that TCS is delivering is operationally ready for the next stage of testing being conducted.

The next stage of testing expected is end to end PSAP NG9-1-1 Deployment Verification testing, starting with a Pilot group of PSAPs identified by TCS’ NG9-1-1 Customer

- XXX Type of Originating 9-1-1 calls that are routed through the NG9-1-1 Network
- PSAPs which has been cut-over to the TCS NG9-1-1 Network

In addition to the TCS Solution being tested, TCS has documented all of the acceptance testing requirements that TCS mandates for other vendors or carriers who will be connecting into the TCS Operated NG9-1-1 Network. TCS will execute a series of tests with each vendor and/or carrier after the vendor and/or carrier proves it has met TCS’ acceptance test requirements.



[12a]

NG9-1-1 Customer

Test Cases for Call Logic Centers

2. PRE testing includes system performance, including voice quality under heavy load and during component failure.
 3. PRE includes a simulated wide-area network including a MPLS network such as what is being deployed by TCS.
- TCS will perform verification testing of the ESINet components and configuration installed to interconnect the Call Logic Centers with each other and with remote PSAPs. This testing is to verify that the network is configured and capable of providing a level of network quality and resiliency that meets the requirements for this project.
 - The Sonus Network verification test plan has been executed (i.e., soft switches).
 - All NG9-1-1 network equipment and connectivity is in place and is configured.
 - TCS test simulation and monitoring equipment is in place.
 - TCS test endpoints are in place.
 - All interoperability-test partners have their environment and/or circuits ready to start interoperability testing and have met the TCS circuit-test acceptance standards for NG9-1-1.

Note The TCS circuit-test acceptance standards for NG9-1-1 are provided as part in a separate document.

1. In this document, "PSAP" means the simulated PSAP test endpoint that TCS is using.
2. In this document, "Originating Call" means the simulated call origination point that TCS is using prior to end to end call flow testing

1.4. For Additional Information

If you have questions about this document, please contact [TCS](#) Client Service Manager for Customer name and contact information]

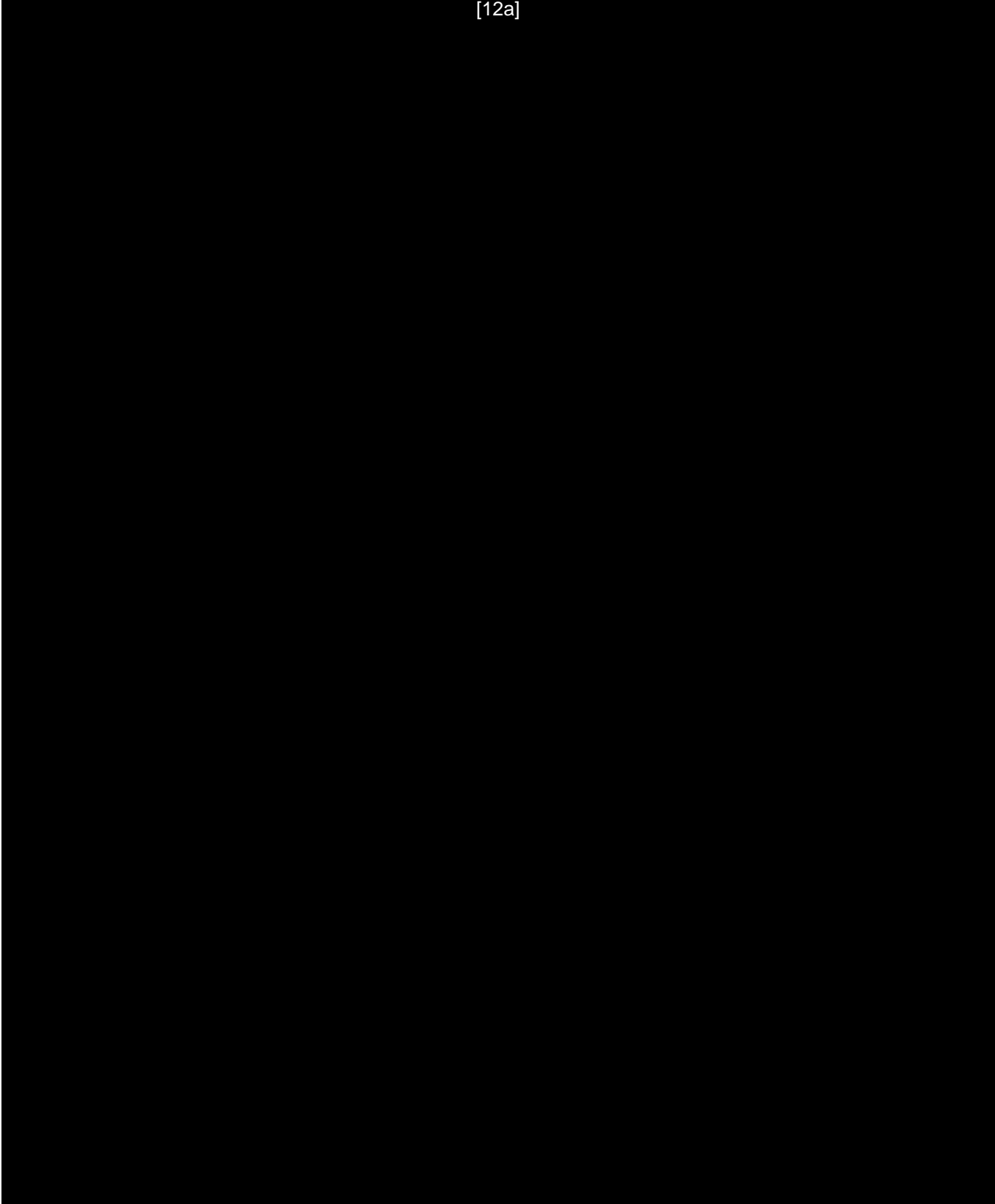
2.6 TCS CLC Hardware Installation

Purpose of this test coverage will be to prove that the redundant power supplies handle power load when plugs are pulled. Additionally this test coverage will prove that network connection redundancy and IP Network Multi Pathing kicks in when expected.



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

[12a]





NG9-1-1 Customer

Test Cases for Call Logic Centers

2.8 TCS NG9-1-1 Selective Routing And Location Applications

Purpose of this test coverage will be to prove that the TCS NG9-1-1 Applications are configured properly and calls route correctly and location data is accurately delivered.

[12a]

NG9-1-1 Customer

Test Cases for Call Logic Centers

	LNG SIPAgentLNG tomcat-xng E2IFProxy CIR
3	Execute following command to verify agents are in running state: rtm status
4	Open xymessage log and verify that only XY 5 and XY 3 are generated during agent start up, no error messages are logged for agent communication, databases connections, etc.
Comments:	



Washington State Military Department
 Next Generation 9-1-1 Emergency Services Internet Protocol Network
 Statement of Work | June 24, 2016

[12a]

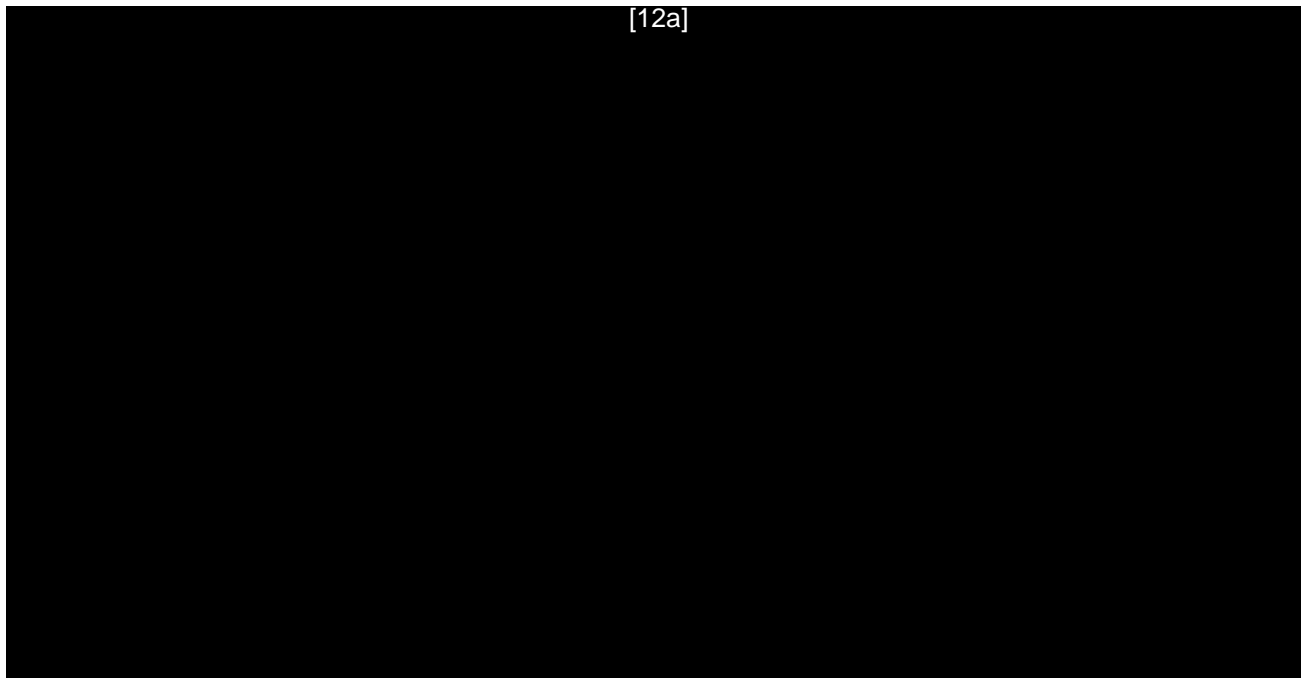
NG9-1-1 Customer

Test Cases for Call Logic Centers

Step #	Method Description
1	Login to server at CLC2
2	Execute following commands to take LNG service down at CLC2 rtm stop -s :ngstate-city2lngsvc1: rtm stop -s :ngstate-city2lngsvc2: rtm stop -s :ngstate-city2lngapp1: rtm stop -s :ngstate-city2lngapp2: rtm stop -s :ngstate-city2cirsvc1: rtm stop -s :ngstate-city2cirsvc2:
3	Execute following command to make sure that LNG service is down at CLC2: rtm status LNG service related agents are in stopped state in the command output
4a	Provision system to route test calls to Legacy PSAP, send a call to SBC, SBC can choose available LNG service at CLC1
4b	Provision system to route test calls to IP enabled PSAP, send a call to SBC, SBC can choose available LNG service at CLC1
5a	Verify Legacy PSAP ALI bid/rebid are successful
5b	Verify IP-enabled PSAP ALI bid/rebid are successful
6	Restore system



[12a]



NG9-1-1 Customer

Test Cases for Call Logic Centers

3. Test Coverage Results Summary

Summary of Test Results: Voice Trunks From WSP	Test Result	Deviation Number ○ Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: ISUP Signaling Associated with NG9-1-1 Calls	Test Result	Deviation Number ○ Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: LEC Link Network into TCS Network	Test Result	Deviation Number <input type="checkbox"/> <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: Administrative, Monitoring and Backhaul Network Connections from TCS Seattle and Phoenix to NEW CLCs	Test Result	Deviation Number <input type="checkbox"/> <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: Back-up Internet Connections from Seattle	Test Result	Deviation Number
--	--------------------	-------------------------



Washington State Military Department
 Next Generation 9-1-1 Emergency Services Internet Protocol Network
 Statement of Work | June 24, 2016

NG9-1-1 Customer

Test Cases for Call Logic Centers

and Phoenix		<input type="radio"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: Administrative, Monitoring and Backhaul Network Connections from TCS Seattle and Phoenix to Customer CLCs	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: TCS Customer CLC Hardware Installation	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: Provisioning API through UAT	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: TCS NG9-1-1 Selective Routing and Location Applications	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:

NG9-1-1 Customer

Test Cases for Call Logic Centers

Test Reviewer:	Signature:	Date:
Summary of Test Results: Monitoring and Alarming Components in the NG9-1-1 Platform	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: ESI NET Connections: MPLS to CLCs	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: ESINET Connections: MPLS to PSAPs	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:

Summary of Test Results: PSAP Equipment	Test Result	Deviation Number <input type="checkbox"/> Applicable?
Test Execution Completion Initial/Date:	<input type="checkbox"/> Pass <input type="checkbox"/> Fail	
Test Engineer:	Signature:	Date:
Test Reviewer:	Signature:	Date:



PSAP Test Plan

Starting on the next page is the foundation of the test plan TCS will use to ensure successful PSAP connectivity to the Washington ESIInet.



TeleCommunication Systems Inc.
2401 Elliott Avenue
Seattle WA 98121
Phone 206 792-2000
Fax 206 792-2001
www.telecomsys.com



Customer NG9-1-1 PSAP Test Plan (Rev7)

PSAP Name Goes Here

Enter Test Date Here

Document Number: TCSP-210

Document Release 7.0

December 2015


The xypoint location platform
from 



Table of Contents

1. Introduction.....	4
1.1. Purpose.....	4
1.2. Assumptions.....	4
2. PSAP test Scenarios.....	5
2.1. Test Scenario 1 - PSAP Operator to answer an incoming call and check call quality Vs legacy network.....	5
2.2. Test Scenario 2 - Validate Policy Routing (Overflow Condition)	7
2.3. Test Scenario 3 - PSAP operator calls back a short duration or abandoned call.....	8
2.4. Test Scenario 4 - NextGen9-1-1 PSAP Transfers a 911 call to a Legacy PSAP.....	9
Verify they can still communicate with 911 caller, and; once Legacy Operator confirms they can still communicate with caller, to transfer call back to NG9-1-1 PSAP	
2.5. Test Scenario 5 - NextGen9-1-1 PSAP Transfers a 911 call to a NextGen9-1-1 PSAP	10
2.6. Test Scenario 6 - Establish communications among the PSAP call taker, 911caller, 3rd party service provider from PSAP equipment	13
2.7. Test Scenario 7 - Validate * codes/ 1-button transfers/manual transfers	14
2.8. Test Scenario 8 - Validate Policy Routing (Alternate Condition)	15
3. Additional validation tests for the PSAP post call through testing	17
3.1 - Validate Recording Capabilities	17
3.2 - Validate Logging Capabilities.....	17
4. Back out Procedure for PSAPS.....	18
5. Summary of Test Results & PSAP Testing Sign Off.....	19
6. PSAP Star (*) code attachment(s).....	20

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 4

1. Introduction

1.1. Purpose

The Purpose of this document is to prepare PSAPS for testing requirements for operation on the Customer NG9-1-1 network.

1.2. Assumptions

PSAPs will meet all the requirements outlined in the PSAP NG preparedness documentation
 Carriers will meet all the requirements outlined in the Carrier to NG preparedness documentation for PSAP testing
 Testing will be performed with ESInet FX lines.
 PSAPs/ECDs will have added new trunk ports and trunk cards as applicable and not reallocated existing trunk capacity to ESInet.



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 5

2. PSAP test Scenarios

2.1. Test Scenario 1 - PSAP Operator to answer an incoming call and check call quality Vs legacy network

Test Case Number:	Test Scenario 1					
Test Case Coverage Area:	All Customer PSAP testing					
Test Stage:	PSAP Testing on NG9-1-1 platform					
Test Case:	PSAP Operator to answer incoming calls and check call quality in comparison to legacy network					
Expected Results:	PSAP Operator answers call and is able to communicate with the 911 caller					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	A 911 test call is initiated via a ESInet FX line	Call routes to the intended PSAP		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.1	NG PSAP operator answers call and verifies Telephone number populates and NRF (No Record Found appears)	Communication established between 911 caller and PSAP operator and CBN and NRF appear		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	Voice Quality is checked: 911 Test Caller speaks	PSAP Operator listens to quality of voice: Do they hear echo on NG9-1-1 line? Do they hear feedback on NG9-1-1 line? Is volume level good? Can they clearly hear call tester?	Echo? Feedback? Volume level? Call clarity?	<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.1	Voice Quality is checked: PSAP Operator speaks	911 caller listen to quality of voice: Do they hear echo on NG9-1-1 line? Do they hear feedback on NG9-1-1 line? Is volume level good? Can they clearly hear PSAP Operator?	Echo? Feedback? Volume level? Call clarity?	<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.2	DTMF Test: 911 Test Caller let's Operator know they will be pressing a digit (9) and asks Operator to move their listening device away from their ear.	PSAP operator to listen to DTMF tone over the NG9-1-1 line. Is DTMF tone signal good?		<input type="checkbox"/> Yes <input type="checkbox"/> No		



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 6

3	Additional 911 test call is initiated to ESInet FX line via legacy trunks (dial 911)	Call routes to intended PSAP	<input type="checkbox"/> Yes <input type="checkbox"/> No		
4	PSAP operator is alerted to calls in queue	PSAP operator can visually identify calls in queue	<input type="checkbox"/> Yes <input type="checkbox"/> No		
5	PSAP operator places test call #1 on hold or if PSAP does not place calls on hold, skips and goes to step 6	Call placed on hold if this step applies	<input type="checkbox"/> Yes <input type="checkbox"/> No		
5.1	PSAP operator answers test call #2 in queue	Communication established between 2nd 911 caller and PSAP operator	<input type="checkbox"/> Yes <input type="checkbox"/> No		
5.2	PSAP operator speaks with call #2 and compares call volume/quality of legacy call to that of the NG call.	PSAP Operator listens to quality of voice: Is call quality/volume level comparable to NG911 call?	<input type="checkbox"/> Yes <input type="checkbox"/> No		
5.3	DTMF Test: Caller #2 let's Operator know they will be pressing a digit (9) and asks Operator to move their listening device away from their ear to compare with DTMF tone of NG call	PSAP operator to listen to DTMF tone over the legacy line to compare with NG911 line. Is DTMF tone signal comparable?	<input type="checkbox"/> Yes <input type="checkbox"/> No		
6	PSAP operator releases #2 call	Call released	<input type="checkbox"/> Yes <input type="checkbox"/> No		
7	PSAP operator examines call #1 for hold time (if step 5 applies)	The elapsed hold time is displayed in call record (if step 5 applies)	<input type="checkbox"/> Yes <input type="checkbox"/> No		
8	PSAP operator waits for system to alert call taker that call #1 is still on hold	After a pre-defined time the system will alert the PSAP operator of caller on hold	<input type="checkbox"/> Yes <input type="checkbox"/> No		
9	PSAP operator selects call #1 and takes the call off hold	PSAP operator can communicate with caller #1	<input type="checkbox"/> Yes <input type="checkbox"/> No		
10	PSAP operator ends call #1	Call disconnects	<input type="checkbox"/> Yes <input type="checkbox"/> No		
Comments:					

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 7

2.2. Test Scenario 2 - Validate Policy Routing (Overflow Condition)

Test Case Number:	Test Scenario 2					
Test Case Coverage Area:	All PSAP Testing					
Test Stage:	PSAP Testing					
Test Case:	Validate NG9-1-1 virtual trunks and CPE connections work as expected, via Alternate Routing Overflow routing testing. PSAP Vendor takes inbound NG9-1-1 trunks to the PSAP down one by one, until all are down.					
Expected Results:	Each NG9-1-1 trunk to PSAP works as expected, until all NG9-1-1 trunks are down and PSAP will enable Alternate and overflow routing					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	PSAP Vendor makes first inbound NG9-1-1 trunk to PSAP busy or ports are disabled from gateway. A 911 test call is initiated via a ESInet FX line. Note: this step repeated for each NG9-1-1 trunk into PSAP, until all trunks are down.	In-bound calls will route via 2nd or next trunk being tested NG9-1-1 trunk to PSAP, PSAP Operator validates communication with 911 caller and expected call data. Note: testing of all NG9-1-1 trunks is noted in actual results. All trunks must pass for this test case to pass.		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	911 test call is initiated to PSAP via a ESInet FX Line	Call attempts to reach PSAP and is diverted to Overflow routing partner		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	Call is routed to Alternate routing partner	Alternate PSAP operator activates a button to accept call		<input type="checkbox"/> Yes <input type="checkbox"/> No		
4	Alternate PSAP operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
5	Alternate PSAP disconnects 911 call	Ready for next Test Scenerio		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6	PSAP Vendor brings all NG9-1-1 trunks back to operational state	Call completed		<input type="checkbox"/> Yes <input type="checkbox"/> No		
Comments:						



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 8

2.3. Test Scenario 3 - PSAP operator calls back a short duration or abandoned call

Test Case Number:	Test Scenario 3					
Test Case Coverage Area:	Pilot PSAP testing only (Non-Pilot Customer PSAPS to test features once live on NG9-1-1 system)					
Test Stage:	PSAP Testing					
Test Case:	Call tester ends call before PSAP can answer to simulate a short duration or abandoned call. PSAP then attempts to call back test caller.					
Expected Results:	PSAP operator sees abandoned or short duration call and follows existing PSAP standards and re-establishes communication with 911 caller.					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	A 911 test call is initiated – Test Caller hangs up immediately after first ring.	Call rings to PSAP and tester hangs up before operator answers call.		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	NG PSAP operator follows short/abandon call procedure) if ALI data verifies telephone or Call Back Number (CBN) populates and valid ALI display per type of call.	PSAP can see CBN of abandoned call		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	PSAP operator activates call back feature	N/A		<input type="checkbox"/> Yes <input type="checkbox"/> No		
4	PSAP operator communicates with caller	The PSAP operator is able to reconnect to the 911 caller	Caller ID of PSAP:	<input type="checkbox"/> Yes <input type="checkbox"/> No		
Comments:						

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 9

2.4. Test Scenario 4 - NextGen9-1-1 PSAP Transfers a 911 call to a Legacy PSAP

Test Case Number:	Testing Scenario 4					
Test Case Coverage Area:	Pilot PSAP testing (optional for all PSAPS)					
Test Stage:	PSAP testing					
Test Case:	NextGen9-1-1 PSAP Transfers a 911 call to a Legacy PSAP. Next Gen9-1-1 PSAP hangs up and Legacy PSAP transfers call back to NextGen9-1-1 PSAP.					
Expected Results:	The Legacy PSAP will receive the call and populate the 911 callers information on their console. Legacy PSAP is able to transfer call back to NextGen9-1-1 PSAP and 911 callers information populates on their console.					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	911 test call is initiated to NG PSAP via a ESInet FX line	911 call routes to intended PSAP		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.1	NG PSAP operator accepts the call	NG PSAP operator can communicate with 911 caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.2	NG PSAP operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	NG PSAP operator determines call should be transferred.	Call is determine to be out of NG PSAP boundary		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.1	NG PSAP operator selects the system transfer option and transfers the 911 caller	Transfer initiated	PSAP Transferred to: *Code used:	<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.2	NG PSAP operator remains on the line for Legacy S/R PSAP operator to accept the 911 call via assisted transfer.	NG PSAP operator remains connected to transferred call		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	Legacy S/R PSAP operator accepts NG911 call transfer	911 call is transferred to correct Legacy S/R PSAP and can communicate with NG PSAP operator and 911 caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3.1	Legacy S/R PSAP operator verifies the Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7) February 23, 2012 Page 10						
4	NG PSAP operator asks Legacy operator to: Verify they can still communicate with 911 caller, and; once Legacy Operator confirms they can still communicate with caller, to transfer call back to NG9-1-1 PSAP	NG operator instructs Legacy PSAP operator of tests to perform.		<input type="checkbox"/> Yes <input type="checkbox"/> No		
5	NG PSAP operator disconnects from call	NG PSAP disconnects and the transferred call doesn't drop		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6	Legacy PSAP operator confirms he/she can still communicate with 911 caller	911 caller remains on the line		<input type="checkbox"/> Yes <input type="checkbox"/> No		
7	Legacy S/R PSAP operator selects the system transfer option and transfers the 911 caller to NG PSAP	Transfer initiated		<input type="checkbox"/> Yes <input type="checkbox"/> No		
7.1	Legacy S/R PSAP operator remains on the line for NG PSAP operator to accept the 911 call	Legacy S/R PSAP operator remains connected to transferred call		<input type="checkbox"/> Yes <input type="checkbox"/> No		
8	NG operator accepts 911 call transfer	911 call is transferred to correct NG PSAP and can communicate with Legacy S/R PSAP operator and 911 caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
8.1	NG PSAP operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
9	Legacy S/R PSAP operator disconnects from call	Legacy S/R PSAP disconnects and the transferred call doesn't drop		<input type="checkbox"/> Yes <input type="checkbox"/> No		
10	NG PSAP confirms he/she can still communicate with 911 caller	911 caller remains on the line		<input type="checkbox"/> Yes <input type="checkbox"/> No		
11	NG PSAP disconnects 911 call	Call completed		<input type="checkbox"/> Yes <input type="checkbox"/> No		
Comments:						



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 11

2.5. Test Scenario 5 - NextGen9-1-1 PSAP Transfers a 911 call to a NextGen9-1-1 PSAP

Test Case Number:	Testing Scenario 5					
Test Case Coverage Area:	Pilot PSAP testing - All PSAPS - Depends on transfer partner PSAP status					
Test Stage:	PSAP testing					
Test Case:	NextGen9-1-1 PSAP Transfers a 911 call to a NextGen9-1-1 PSAP					
Expected Results:	The NG PSAP will receive the call and populate the 911 callers information on their console					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	911 test call is initiated to NG PSAP via a ESInet FX line	911 call routes to intended PSAP		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.1	NG PSAP #1 operator accepts the call	NG PSAP operator can communicate with 911 caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.2	NG PSAP #1 operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.3	NG PSAP #1 operator determines call should be transferred.	Call is determine to be out of NG #1 PSAP boundary		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	NG PSAP #1 operator selects the system transfer option and transfers the 911 caller to NG PSAP #2 either via *code or manual transfer	Transfer initiated	PSAP Transferred to: *Code or number used:	<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.1	NG PSAP #1 operator remains on the line for NG PSAP #2 operator to accept the 911 call	NG #1 PSAP operator remains connected to transferred call		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	NG #2 operator accepts NG911 call transfer	911 call is transferred to correct NG PSAP and can communicate with NG #1 PSAP operator and caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3.1	NG PSAP #2 operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
4	NG PSAP #1 operator disconnects from call	NG #1 PSAP disconnects and the call remains up		<input type="checkbox"/> Yes <input type="checkbox"/> No		

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 12

5	NG PSAP #2 confirms he/she can still communicate with 911 caller	Caller remains on the line		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6	OPTIONAL: If *code exists for NG PSAP #2 to transfer back to NG PSAP #1, NG PSAP #2 to transfer back to NG PSAP #1. Else – continue to step 7.	Transfer initiated		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6.1	NG PSAP #1 operator accepts NG911 call transfer	911 call is transferred to correct NG PSAP and can communicate with NG PSAP #2 operator and caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6.2	NG PSAP #1 operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6.3	NG #2 operator drops off the call	NG PSAP #2 disconnects and the transferred call doesn't drop		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6.4	NG #1 operator drops off the call	Call completed		<input type="checkbox"/> Yes <input type="checkbox"/> No		

Comments:



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 13

2.6. Test Scenario 6 - Establish communications among the PSAP call taker, 911 caller, 3rd party service provider from PSAP equipment

Test Case Number:	Test Scenario 6					
Test Case Coverage Area:	All PSAP Testing					
Test Stage:	PSAP Testing					
Test Case:	Establish communications among the PSAP call taker, 911 caller, 3rd party service provider from PSAP equipment					
Expected Results:	Enables PSAP call taker to establish conference sessions with other entities as required. The PSAP call taker initiates a conference session. The PSAP call taker will stay on the line with caller and dispatcher to assist the caller and the dispatcher.					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	911 test call is initiated to PSAP by via a ESInet FX line	Call routed to PSAP		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.1	PSAP operator receives the call	PSAP operator communicates with 911 caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	PSAP operator chooses conference call option	PSAP system provides conferencing option		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.1	PSAP operator initiates call to another entity outside PSAP system	PSAP system indicates conference call		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.2	PSAP operator verifies second entity answers and that the first caller and other entities can hear each other	PSAP operator verifies communication has been established with additional entity		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.3	PSAP operator places call on hold via workstation	Verifies remaining two parties can still talk to each other		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.4	PSAP operator rejoins the call and places original caller on mute	Verifies that caller cannot hear the PSAP operator and 3rd party		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2.5	PSAP operator re-engages with all callers and ends the call	PSAP operator confirms communication has been re-established between all parties		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	PSAP operator verifies conference call displays in call records	Details of the call reflect in the PSAP system call record log		<input type="checkbox"/> Yes <input type="checkbox"/> No		
Comments:						



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 14

2.7. Test Scenario 7 - Validate * codes/ 1-button transfers/manual transfers

Test Case Number:	Test Scenario 7
Test Case Coverage Area:	All PSAP Testing
Test Stage:	PSAP Testing
Test Case:	Validate * codes/ 1-button transfers
Expected Results:	PSAP pressed each star code programmed on its CPE and call either transferred to another PSAP and/or to a non PSAP entity such as Poison Control. Will note each star code programmed for PSAP and which PSAP and/or non PSAP entity call reached when star code pressed.

Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	911 test call is initiated to PSAP via a ESInet FX Line	Call routed to PSAP		<input type="checkbox"/> Yes <input type="checkbox"/> No		
1.1	PSAP operator receives the call	PSAP operator communicates with 911 caller		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	PSAP Operator presses star code # for	Call transferred to correct star code transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	PSAP Operator presses star code # for	Call transferred to correct star code transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
4	PSAP Operator presses star code # for	Call transferred to correct star code transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
5	PSAP Operator presses star code # for	Call transferred to correct star code transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6	PSAP Operator presses star code # for	Call transferred to correct star code transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
7	PSAP Operator performs manual transfer using 7-digits	Call transferred to correct transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
8	PSAP Operator performs manual transfer using 10-digits	Call transferred to correct transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
9	PSAP Operator performs manual transfer using 11-digits	Call transferred to correct transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		
10	Optional: PSAP Operator performs manual transfer using 8 and 12-digits ***Only applicable, if PSAP	Call transferred to correct transfer point		<input type="checkbox"/> Yes <input type="checkbox"/> No		



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 15

<i>requires 9 to get outside line***</i>						
11	Verify DTMF Pass through on Transfer / Conference	Transfer / Conference to 3 rd party agency that uses IVR option system (TSP, Language Line) and confirm that PSAP operator can navigate menu with DTMF tones		<input type="checkbox"/> Yes <input type="checkbox"/> No		
Comments:						

2.8. Test Scenario 8 - Validate Policy Routing (Alternate Condition)

Test Case Number:	Test Scenario 8					
Test Case Coverage Area:	All PSAP Testing					
Test Stage:	PSAP Testing					
Test Case:	Validate Alternate Routing					
Expected Results:	PSAP will enable Alternate and overflow routing					
Step	Test Procedure	Expected Result/Value	Actual Result/Value	Expectation Met?	Tested by	Tested on (mm/dd/yy)
1	ESInet Provider disables ESInet connection to PSAP	In-bound calls will enter overflow mode		<input type="checkbox"/> Yes <input type="checkbox"/> No		
2	911 test call is initiated to PSAP via a ESInet FX Line	Call attempts to reach PSAP and is diverted to Alternate routing partner		<input type="checkbox"/> Yes <input type="checkbox"/> No		
3	Call is routed to Alternate routing partner	Alternate PSAP operator activates a button to accept call	PSAP reached:	<input type="checkbox"/> Yes <input type="checkbox"/> No		
3.1	Alternate PSAP operator verifies Telephone number populates and NRF (No Record Found appears)	CBN and NRF		<input type="checkbox"/> Yes <input type="checkbox"/> No		
4	Alternate PSAP disconnects 911 call	Call completed		<input type="checkbox"/> Yes <input type="checkbox"/> No		
5	ESInet Provider places PSAPs ESInet connections back to normal.	Call routes to the intended PSAP – PSAP Operator/Vendor verifies calls over NG-1-1 trunks		<input type="checkbox"/> Yes <input type="checkbox"/> No		
6	911 Tester places test call to verify NG9-1-1 trunks all back in order	Call routed to PSAP		<input type="checkbox"/> Yes <input type="checkbox"/> No		

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 16

Comments:					
-----------	--	--	--	--	--



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 17

3. Additional validation tests for the PSAP post call through testing

3.1 - Validate Recording Capabilities

Test Case Number	PSAP System Capability Test Scenario #1
Test Case Coverage Area:	PSAP CPE Only
Test Stage:	Recommended Additional PSAP System Tests
Test Case:	Validate Recording Capabilities
Expected Results:	Obtain test session information to verify recording functions properly post ESInet transition
Comments:	

3.2 - Validate Logging Capabilities

Test Case Number	PSAP System Capability Test Scenario #2
Test Case Coverage Area:	PSAP CPE Only
Test Stage:	Recommended Additional PSAP System Tests
Test Case:	Validate Logging Capabilities
Expected Results:	Obtain test session information to verify recording functions properly post ESInet transition
Comments:	

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 18

4. Back out Procedure for PSAPS

Test Case Number:	Back Out Procedure		
Test Case Coverage Area:	All PSAPs		
Test Stage:	PSAP testing does not Pass		
Test Case:	Backing out of cut over to NG 911 system		
Expected Results:	It was identified prior or during testing that: a) PSAP did not meet all of their requirements for testing B) a wireless carrier did not meet all their requirements to complete testing or C) calls are not routing and/or data not available as expected. TCS logs a pre-Go Live trouble ticket to document trouble(s) encountered during testing.		
Step	Test Procedure	Expected Result/Value	
1	Do all parties agree that PSAP can go live?	<input type="checkbox"/> Yes – Proceed to step 9 <input type="checkbox"/> No – Proceed to step 2	
2	Do PSAP, TCS and Vendors agree that a roll back to the Legacy S/R is required or is there an outstanding issue keeping the PSAP from going live?	<input type="checkbox"/> Rollback to Legacy S/R. Proceed to step 3 <input type="checkbox"/> Network stays up, but outstanding issues keep from going live. Proceed to step 5	Describe issue keeping PSAP from going live:
3	CPE Vendor begins roll back at PSAP	Disconnects ESInet DS-1 connections	
4	CPE Vendor will remove the trunk cables from the ESInet gateway devices and reconnect CPE Trunk cards to the Legacy S/R	Vendor completes manual (and or virtual) change of the trunks	
5	In conjunction with Step 2, ESInet provider will enable routes to the Legacy S/R (Hairpin method)	911 calls are being sent to the Legacy S/R	
6	911 test calls are initiated to PSAP to ensure legacy S/R path is functioning	Call received at PSAP, each trunk line is validated	
7	TCS notes outstanding issue and creates an incident ticket	Assignment of trouble for resolution. Incident #	TCS to send test results document to all parties noting the current PSAP status.
8	Once outstanding issues have been resolved, Incident ticket is closed.	PSAP is cleared to go live.	Describe steps taken to resolve issues:
9	PSAP is now live on ESInet	TCS to send go-live notification	
Comments:			



TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 19

5. Summary of Test Results & PSAP Testing Sign Off

Summary of Test Results for (Name, county and state of PSAP tested):			
Total number of test calls made:			
Test Execution Completion Initial/Date:	<input type="checkbox"/> PASS	Test Host: _____	Date: _____
Test Date:	<input type="checkbox"/> FAIL	Test Reviewer: _____	Date: _____
Go-Live Date:			

PSAP Authority:	
Signature:	Date:
Company:	

TCS Client Services Manager:	
Signature:	Date:
Company:	TCS

Test Host:	
Signature:	Date:
Company:	TCS

TCS - Customer NG9-1-1 PSAP Test Plan (Rev7)
 February 23, 2012
 Page 20

6. PSAP Star (*) code attachment(s)

From ESInet and/or PSAP Vendor (required attachment if PSAP chooses not to test all their star codes)



11.1.22. Trouble Escalation Procedures – [RFP 6.1.23]

In addition to the outage notification and reporting requirements identified elsewhere within this document, Successful BIDDER shall be required to provide, as part of Stage 5, escalation procedures which include contact information (Name, telephone number, hours) for each level of escalation. All procedures (and identified contacts) must accommodate the real-time 365X24X7 nature of 9-1-1.

We take great pride in ensuring customers receive notifications in a timely manner. The escalation table in Exhibit 135 lists resources available to Washington should unique situations arise that warrant an escalation. Additional contact information will be provided in Stage 5.

Exhibit 135. Escalation Resources

Escalation	Group	Title	Telephone Number
	Network Operations Center	Network Operations Center	[12a]
1st Escalation	Network Operations Center	Supervisor, NOC Monitoring (Tier 1)	
2nd Escalation	Network Operations Center	Manager, Tier 2 ATAC	
3rd Escalation	Network Operations Center	Director, NOC Services	
4th Escalation	Safety & Security Group	Vice President, Service Delivery	

11.1.23. Outage Notification Process – [RFP 6.1.24]

BIDDERS shall identify the Outage Notification process that is used internally within the BIDDERS organization i.e., all the steps and/or departments involved prior to notifying MIL.

TCS has a robust notification process that accommodates the Agency’s need. On outages that result in the inability to deliver calls, an alarm condition will be raised and NOC troubleshooting and notification processes will ensue. The TCS [12a] technical support tiers and responsibilities are:

- Tier 1: NOC
 - Incident detection and management
 - Incident triage and troubleshooting
 - Resolution or escalation of issues that cannot be resolved in a timely manner
- Tier 2: Advanced Technical Assistance Center (ATAC)
 - 24x7 application subject matter experts (SMEs)
 - In-depth troubleshooting and analysis
 - Resolution of call-quality errors
- Tier 3: Operations Engineering



- 24x7 network engineers/system engineers
- Tier 4: Software engineering
- 24x7 software development

Assuming time allows, and dependent on the nature of the event, we expect the first two NOC tiers to be involved in troubleshooting prior to any outage notification.

As shown in Exhibit 136, TCS sends at least three color-coded notifications for each NOC event.

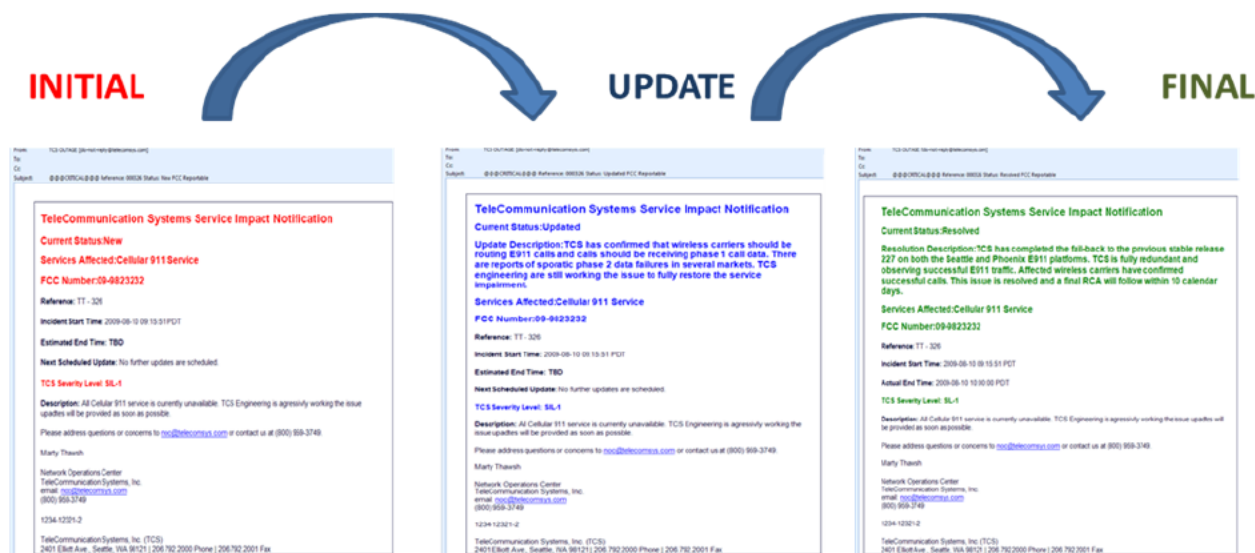


Exhibit 136. NOC Event Notification Process

The final NOC notification report will contain a summary of the event to serve as the incident report. A formal RCA will follow [12a].

Events that require notifications will first be via a phone call and then followed-up with an email to the PSAPs, and the Agency will be notified by sending an email [12a]. [redacted] should access to email be unavailable.

TCS will notify the customer by phone or email, using the most current contact information on file for the customer. All communications sent to the customer by TCS will include the TCS trouble ticket number.



Exhibit 137. SIL Table

Severity Level	Description	Notification	Target Resolution
<p>1 – Critical</p>	<ul style="list-style-type: none"> Mission-critical functionality is lost, rendering the entire system inoperable. Involves critical impacts on the system, such as a loss of 50% or more of call-taking capacity of the system or complete loss of a critical functionality of the system (e.g., no delivery of either Automatic Number Identification [ANI] or ALI). 	<ul style="list-style-type: none"> Initial response to PSAP occurs, via phone, as soon as possible [12a] after incident identification. Subsequent updates occur hourly via phone and/or email. 	<ul style="list-style-type: none"> Code correction or patch by TCS, or a procedure for customer to bypass or work around the anomaly in order to continue operations; [12a] If bypass or work-around is provided, TCS shall continue good faith resolution efforts to create a code correction or patch for customer. Code correction or patch details will be shared with customer.
<p>2 – High</p>	<ul style="list-style-type: none"> Major failure or loss of functionality of components or features of the system, but the system itself remains operable. Involves substantial impact to call-taking or other major system functionality (e.g., no delivery of either ANI or ALI, for a particular class of service). 	<ul style="list-style-type: none"> Initial response to PSAP occurs, via phone, as soon as possible [12a] after incident identification. Subsequent updates occur at least every 12 hours via phone and/or email. 	<ul style="list-style-type: none"> Code correction or patch by TCS, or a procedure for customer to bypass or work around the anomaly in order to continue operations; [12a] If bypass or work-around is provided, TCS shall continue good faith resolution efforts to create a code correction or patch for customer. Code correction or patch details will be shared with customer.



Severity Level	Description	Notification	Target Resolution
3 – Medium	<ul style="list-style-type: none"> Noncritical system failure that causes performance degradation or system components to malfunction. Reported problems disabling specific nonessential functions; error condition is not critical to continuing operations and/or workaround has been determined for the error condition. 	<ul style="list-style-type: none"> Initial response to PSAP, via email, within [12a] business hours. Service during normal business hours (8 a.m. to 5 p.m. EST Monday through Friday). 	<ul style="list-style-type: none"> Workaround or temporary fix within less [12a] Code correction in the next regular update or maintenance release. If bypass or workaround is provided, TCS shall continue good faith resolution efforts to create a code correction or patch for customer. Maintenance release details will be shared with customer.
4 – Low	<ul style="list-style-type: none"> Minor or cosmetic issue to the system, but the core functionality of the system is not significantly affected. Involves a loss of a minor functionality of the system or incorrect operation of a minor functionality of the system. 	<ul style="list-style-type: none"> Initial response to PSAP, via email, [12a] business days. Service during normal business hours (8 a.m. to 5 p.m. EST Monday through Friday). 	<ul style="list-style-type: none"> Code correction in the next regular update or maintenance release. If TCS is unable to provide a code correction in a future update or maintenance release using commercially reasonable efforts, TCS will use commercially reasonable efforts to provide a workaround solution to customer.

11.1.24. System Documentation – [RFP 6.1.25]

BIDDER shall provide documentation that describes the overall system architecture, including system diagrams; element operations and associated call flows. In addition, documentation shall include lifecycle, disaster and change management process/procedures.

We will fully document all system architecture and call flow diagrams once finalized with the Agency. These documents will describe architecture, systems and their operations, and various call flow scenarios. Given the extensive nature of that documentation, we’ve only included examples of the overall documentation set here. For example, a high-level view of our architecture is shown in Exhibit 138. This exhibit illustrates the demarcation points between various functions of the ESInet, including TDM ingress, call routing applications, and monitoring infrastructure. Each generalized function is connected via highly available and redundant IP circuits. This diagram serves as a logical overview of the system and would be complemented by more in-depth diagrams and documentation.



[12a]

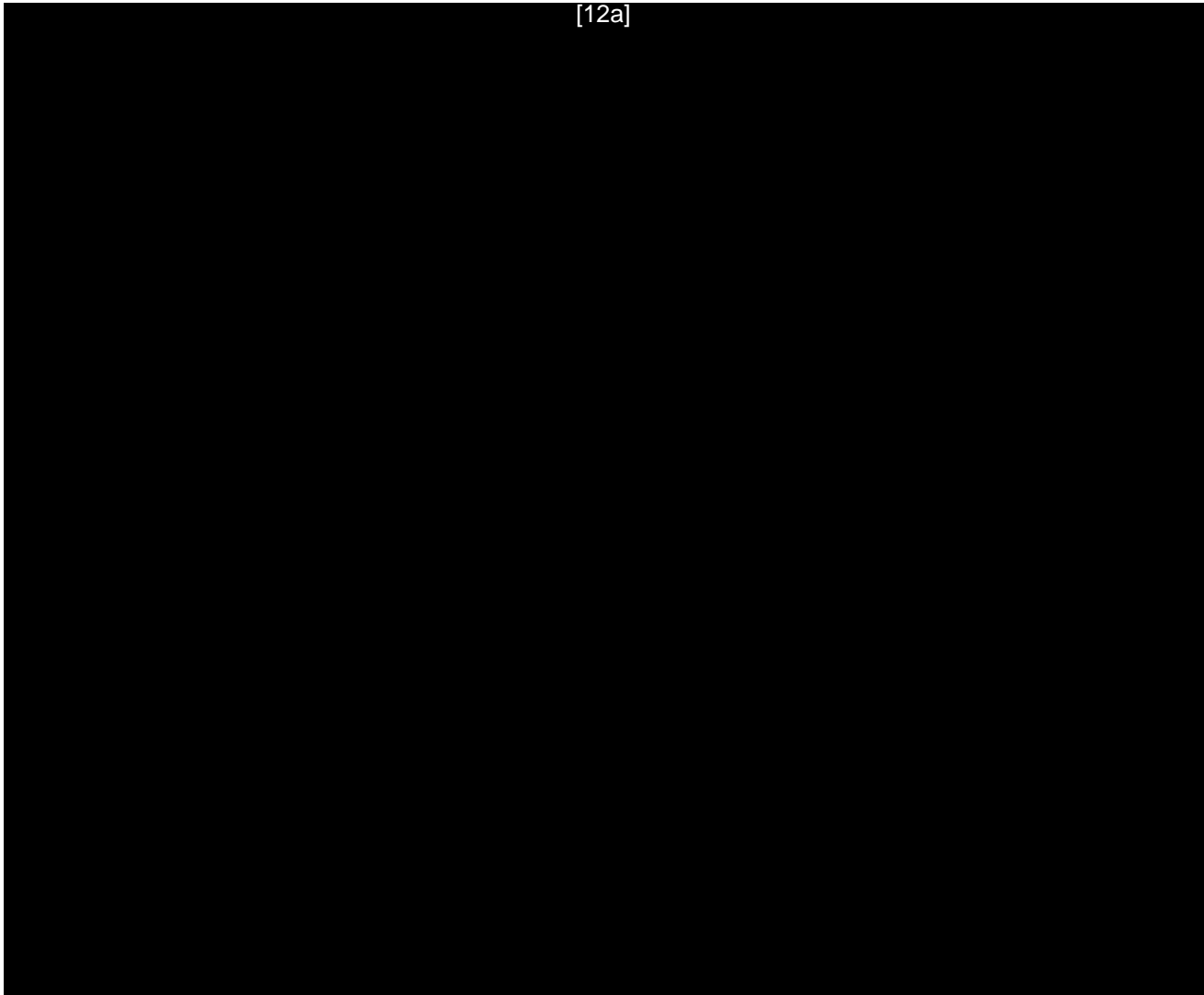


Exhibit 138. High-Level View of TCS Hosted NG9-1-1 Architecture



TCS has established standardized disaster recovery plans for all of its systems. Process documentation is illustrated by the Disaster Recovery Plan table of contents shown in Exhibit 139.

Disaster Recovery Plan		Disaster Recovery Plan	
Table of Contents			
1. Introduction.....	1	9. Disaster Recovery Tools and Procedures.....	22
1.1. Scope.....	1	9.1. Disaster Recovery Cabinet.....	22
1.2. Audience.....	1	9.2. Functional Area Recovery Concepts.....	22
1.3. Purpose.....	1	10. Team and Worksite Recovery Checklists.....	26
1.4. Assumptions.....	1	11. Appendix A – Disaster Recovery Testing Checklist.....	30
1.5. Objectives.....	2		
2. Disaster Recovery Policy.....	4		
2.1. Building Security.....	4		
2.2. Employee Safety.....	4		
2.3. Loss Prevention.....	4		
2.4. Vital Records.....	5		
2.5. Vendor and Customer Disaster Considerations.....	5		
2.6. Document Change Management.....	5		
2.7. Training.....	6		
2.8. Disaster Recovery Team Responsibilities.....	7		
2.9. Disaster Recovery Testing and Plan Maintenance.....	8		
2.10. Communication TCS.....	8		
2.11. Communication with External Parties.....	9		
3. Recovery Strategy and Time Objectives.....	10		
3.1. Recovery Strategy.....	10		
3.2. Recovery Time Objectives.....	12		
4. System Recovery Prioritization.....	13		
4.1. System Restoration Prioritization.....	13		
5. Systems and Personnel Management.....	15		
5.1. Systems Configuration.....	15		
5.2. Personnel List.....	15		
5.3. Vendor and Customer Contact List.....	15		
5.4. Network Access.....	15		
6. Data Loss Prevention.....	16		
6.1. Access to Off-site Backup Data.....	16		
7. Disaster Recovery Plan Testing and Maintenance.....	18		
7.1. Test Objectives.....	18		
7.2. Test Structure.....	18		
7.3. Test Schedule.....	18		
7.4. Test Administration.....	19		
8. Disaster Declaration.....	20		
8.1. Disaster Declaration Guidelines.....	20		
8.2. Disaster Recovery Teams.....	21		
8.3. Disaster is Declared.....	21		
		List of Tables	
		Table 2-1: Disaster Recovery Training Team Roles.....	6
		Table 2-2: Disaster Recovery Management Team Roles and Responsibilities.....	7
		Table 3-1: Disaster Recovery Timetable for Critical Functions.....	12
		Table 4-1: One-Hour Priority Tasks.....	13
		Table 4-2: One-Day Priority Tasks.....	13
		Table 4-3: Five-Day Priority Tasks.....	14
		Table 6-1: System Backups.....	16
		Table 10-1: Activate the Disaster Teams Checklist.....	26
		Table 10-2: Establish Call Delivery and Monitoring Services Checklist.....	27
		Table 10-3: Recover One-Day Services Checklist.....	28
		Table 10-4: Recover Five-Day Services Checklist.....	29
		List of Figures	
		Figure 1: Disaster Recovery Test Process.....	19
Copyright 2005 Telecommunication Systems Inc. All Rights Reserved. ENG-1102 / TCSV156 Internal Use Only Version 6.5		Copyright 2005 Telecommunication Systems Inc. All Rights Reserved. ENG-1102 / TCSV156 Internal Use Only Version 6.5	

Exhibit 139. Table of Contents from TCS' Established Disaster Recovery Plan

Logical Call Flow documentation is shown by the text-to-911 example shown in Exhibit 140. This diagram is an example of the logical connections that exist in our text solution. Carrier connections are shown on the left, PSAP operations on the right, and the applications connecting these two groups in the middle.



[12a]



Exhibit 140. Logical Call Flow Documentation for Text-to-911

Lifecycle management is included in our solution as part of the service offered to Washington. All patch management activity, end-of-life replacement solutions, and other similar events are managed via our change control process and will be transparent to users of our service.

11.2. ESInet (Core) Requirements [RFP 6.2]

While MIL is steadfast in our desire to achieve full i3 compatibility as quickly as possible, it also understands that many transitional elements will need to be retained until all PSAPs upgrade to full IP functionality AND location information is delivered with each call presented to the ESInet. Figure 5 (redundancy not illustrated) depicts the NG9-1-1 Architecture required to meet the near and long-term requirements of our constituents and providers.

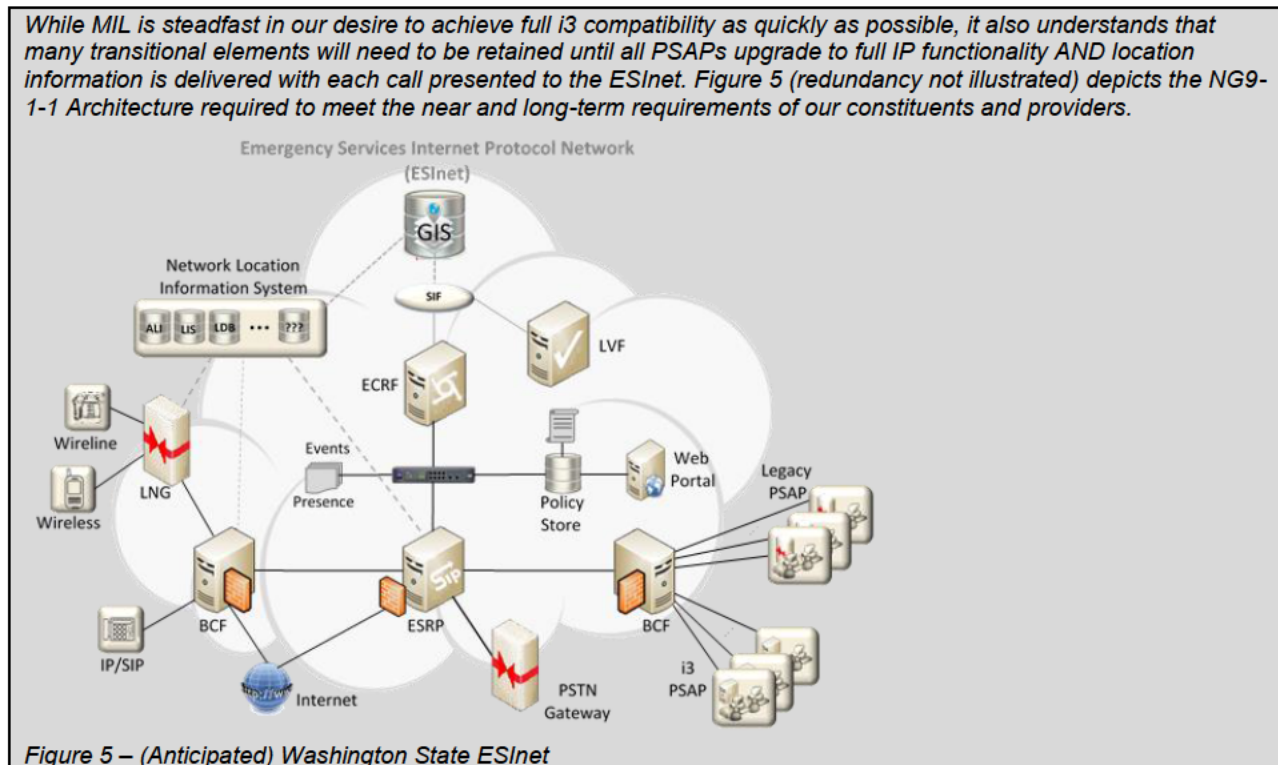


Figure 5 – (Anticipated) Washington State ESInet



TCS has designed the statewide ESInet to meet the near- and long-term requirements of Washington's constituents and providers.

As required, NENA i3-compliant LPGs will be deployed on the ESInet to facilitate initial call delivery and call transfers from the ESInet to legacy PSAPs. These gateways are similar in capability to the LNG/LSRG in terms of protocol conversion (SIP-to-TDM). They also offer functions that help the PSAP retrieve ALI information – even if it is delivered in the form of a PIDF-LO – to facilitate both inter- and intra-ESInet call transfers by using the ECRF. [12

a]

All these ESInet transactions are facilitated by the LPG NG9-1-1 Specific Interworking Function and Location Interworking Function (NIF and LIF, respectively) on behalf of the legacy PSAP.

The LIF function within the LNG is responsible for obtaining location from the ALI, LDB, or LIS/ADR related to the market associated with the call. The LIF will use the E2 interface to query an (MPC)/Gateway Mobile Location Center (GMLC) directly when a call ingresses from a MSC, to obtain wireless location information for location updates compliant with RFC 4119 as updated by RFC 5491 and RFC 5222.

The NIF function is responsible for creating the SIP signaling and managing the SIP interface between the LNG/LSRG and the BCF to the ESRP. First, it determines the correct ANI as sent from the PIF and pass that to the LIF for location querying. The NIF also applies default routing to the next hop should the resulting Uniform Resource Identifier (URI) not be available or for any other failure scenario. The NIF applies any available additional data information about the call.

The functions outlined for both the NENA i3 LNG and the proposed LSRG for transition and interaction with legacy SRs are supported within this proposed platform.

11.2.1. ESInet Infrastructure – [RFP 6.2.1]

The ESInet infrastructure shall be an open standards based (NENA i3), private, secure, extensible, managed and highly available IP network. The infrastructure, routing of packets and services provided within, must support both IPv4 and IPv6. Dual stack implementations are required unless responses provide detailed explanations as to how the solution will eliminate the security issues associated with IP tunnels and TRT. The infrastructure shall incorporate, in compliance with the relevant NENA standards, the following elements/functions:

- LNG
- BCF
- ECRF
- ESRP
- LVF (optional)
- PSTN/TDM Gateway (Optional)
- Legacy PSAP Gateway (LPG) (not illustrated)
- Network Location Information Services (NLIS)
- Internet Gateway (optional)



As stated in Section 6.1, MIL does not require that any of the elements/functions be implemented as separate network elements. However, MIL does require that each element/function provide the NENA specified interface between the elements/functions to enable interworking with different vendor implementations .

[12a] is an open standards-based, NENA i3-compliant, private, secure, extensible, managed and highly available IP network.

11.2.2. Network Location Information Service (NLIS) – [RFP 6.2.2]

As experienced BIDDERS will be aware, full i3 compliance is to a significant degree dependent upon some functions that are external to the ESInet (e.g., LIS). Further, NENA documentation describes the “end-state” and does not fully describe transitional mechanisms. As such, MIL is looking for experienced BIDDERS to provide functionality that will provide the appropriate location information (i3 or Legacy) required by any ESInet element to perform its intended function (e.g., civic address validation , initial routing, dereferencing, etc.). The functionality does not have to be centralized as implied by Figure 5; BIDDER solutions which distribute functionality are acceptable.

Rather than specify detailed requirements as to the required elements (existing or new) and procedures necessary to provide this capability, MIL is leaving it to the BIDDER’s experience on how this shall be accomplished. BIDDER’s proposal shall include detailed documentation as to the elements, interfaces and procedures involved in the provisioning of this capability. MIL expects that the BIDDER will attempt to preserve i3 principles and elements, and shall also identify, to the extent possible, any incompatibilities and/or issues when the Originating Network becomes capable of providing accurate location information with each and every 9-1-1 call.

TCS believes that one unstated benefit of the modular architecture of the NENA i3 ESInet is that, in the future when IP is used end to end, functional components such as the LSRG, LNG and LPG will no longer be required and can be decommissioned without a major upgrade to deployed ESInets. The [12a] ESInet follows the NENA modular design. As a result, elements such as the LNG/LSRG and LPG encapsulate the transitional functionality to allow legacy to interwork with i3 and vice versa.

The LSRG/LNG supports the capability to HTTP-enable an ALI/location database (LDB) whether it is TCS’ [12a] ALI or some other vendor’s. In support of this capability, INVITES leaving the LNG/LSRG toward the ESRP are NENA i3 compliant and contain a geolocation header with Location by Value (LbyV) or Location by Reference (LbyR) Uniform Resource Locator (URL)/Uniform Resource Identifier (URI).

The LPG provides the reverse function for a legacy Centralized Automatic Message Accounting (CAMA) PSAP, enabling the PSAP to receive calls and retrieve ALI from the [12a] ESInet.

Given independent timelines of the origination network (carrier) and the PSAP to become i3 compliant (meaning call delivery/acceptance using SIP INVITE that contains location and call data), TCS understands the need for an NLIS.

To complicate timelines further, wrapped up in the timeline for a PSAP to become i3 compliant is the critical dependence on reliable (98 percent error free) GIS data. As a result, TCS proposes the following plan for the NLIS:

1. At the outset, we can use the existing ALI service provider while the state works to make its GIS NG9-1-1 ready by creating site structure address points. LDB functionality is provided via the [12a] ESInet LNG/LSRG LIF.
2. Transition to [12a] ALI, which allows the state to vet every ALI record against the coalesced GIS site structure address point layer; continue to produce MSAG by using the GIS data as the single source of truth.



3. Cutover to [12a] ALI once the GIS error rate is less than or equal to 2 percent. The [12a] LVF and ECRF would then be available for address validation and call routing. LDB functionality would continue to be available via the [12a] ESInet LNG/LSRG LIF.
4. Eventually it may become desirable to transition to the full NG9-1-1 architecture of Location Information Server (LIS)/Call Information Database (CIDB), but we expect this to be outside of the initial CONTRACT term.

[12a]

The following are the minimum Mandatory requirements.

11.2.2.1. NLIS Availability – [RFP 6.2.2.1]

All elements that may comprise the NLIS, or functional equivalent(s), shall be deployed in a manner that affords 5-9's of Availability. At a minimum the NLIS functionality (or composite elements if distributed) must be deployed in at least two (2) geographically diverse sites.

We will provision the NLIS functional elements in at least [12a] to create a highly available design. As noted above, some of the functionality is resident to the LIF element, which is already deployed in such a manner to accommodate high availability within the LNG/LSRG functional element.

7.2.2.2. NLIS Support for Legacy ALI – [RFP 6.2.2.2]

While PSAPs within the state are in the process of upgrading to i3 CPE, some PSAPs may not be upgraded until after the new i3-based network is in place. As such, the NLIS system must incorporate an ALI database that is compatible with the existing data formats and query mechanisms.

Ownership of all ALI data compiled will remain with the County 911 Authority and no restrictions and/or charges shall be incurred by the County 911 Authority or agency for accessing or obtaining copies of this data for administrative purposes or incorporation into other systems.

SOIs will be sent to the contractor (i.e., successful Bidder) who will function as a Data Base Management System Provider (DBMSP) as defined by NENA. As such, the (originating) Service Provider is responsible for submitting SOI(s) and the DBMSP for loading and any subsequent maintenance.

Note: If necessary the Successful BIDDER will be provided with a complete (and current) electronic copy of the existing ALI database.

The initial database used in the NLIS design will be the ALI database, which is compatible with the existing data formats and queries. As long as the state elects to use the TCS [12a] ALI service, there will be no restrictions or charges incurred by accessing the data. Our view is that the data in the ALI is owned by the 9-1-1 authorities, and as such the 9-1-1 authority should never incur a charge for access to its own data.

Our [12a] ALI service will serve as the DBMS. [12a] ALI accepts SOI loads from the originating service providers and provisions them against the MSAG database. Any fallout in the SOI process is returned to the originating service providers (OSPs) for correction. All successfully validated SOI loads will then be provisioned into the ALI database. In this manner the NLIS system incorporates an ALI database as well as an ALI management system. Both are accounted for in our ALI service.



7.2.2.3. NLIS Documentation – [RFP 6.2.2.3]

At a minimum NLIS, or functional equivalent, documentation shall include:

- *Internal elements (location databases such as LIS, ALI, etc.)*
- *i3 interfaces , including Protocol used*
- *non-i3 interfaces, including Protocol used*
- *Basic operation overview*
- *Data Management processes and procedures,*
 - o *Initial creation of dataset(s)*
 - o *Maintenance of Dataset(s) (new records, deletions, etc.)*

The initial database in the NLIS system will be the ALI database. Other location information will be added as needed. These databases will be accessed by enabling the interfaces to use i3 signaling and protocols. In some cases these interfaces will be natively i3, but in others we will enable legacy signaling and/or allow legacy interfaces to communicate with the databases. Given that the nature of the NLIS is a transitional element, we expect that both legacy and i3 interfaces will be needed throughout the term of the contract.

Upon contract award and after subsequent data-gathering activities we will complete our documentation of the existing legacy interfaces and support as well as i3 interfaces to be used. This documentation is critical in maintaining the processes used in creating and maintaining the initial datasets. We have produced similar documentation for other customers of similar size and complexity, which has illustrated the need for clear processes and procedures.

7.2.3. Legacy Network Gateway (LNG) Originating Network Interconnection – [RFP 6.2.3]

Within the state of Washington, wireline, wireless and VoIP Originating Network Emergency Service (ES) circuits terminate upon LNGs, provided by CenturyLink, and are located in Spokane, Yakima, Seattle and Tukwila.

While NENA 08-003 lays out the framework for an i3 version of an LNG, MIL is not requiring that BIDDERS comply with the internal architecture and how the functional components (i.e., PIF, NIF and LIF) interface with each other. Rather, MIL only requires that the external interfaces comply with the respective NENA requirements. Further, as 1) it is not anticipated that the Washington State ESNet will require hierarchical ESRPs, and 2) the internal functions of an ESRP are (currently) out-of-scope in i3 ; it may be more efficient and economical to locate this functionality within the ESRP. As such MIL has made provision for BIDDERS to locate this functionality (and associated interfaces) either within the LNG or the ESRP at their discretion.

BIDDERS should also consider the requirement(s) of Section 6.2.18.2 when considering the LNG requirements.



To deliver required interworking with legacy systems, the TCS solution provides the LNG and the LSRG. The LNG/LSRG is further divided between the Protocol Interworking Function (PIF), located locally, and the NG9-1-1-Specific Interworking Function (NIF) and LIF, both of which are located in the CLCs. These interfaces provide connections to the legacy E9-1-1 systems and act as gateways into the NG9-1-1 system. As can be seen in Exhibit 141 below, the LNG/LSRG is used for the initial location query as well as the initial routing to the ESRP.

[12a]



Exhibit 141. Call Flow Diagram

The proposed [12a] LNG provides LbyV, populating the Presence Information Data Format – Location Object (PIDF-LO) within the SIP messaging with the full location of the caller via interaction with either the legacy ALI DBMS, during transition, or NLIS infrastructure once that element has been implemented. This interaction complies with the NENA i3 standard. Also, [12a] will be capable of submitting queries to a NENA i3-compliant external LIS and to the required BCF to secure such interconnectivity and subsequent messaging. Furthermore, [12a] can provide location using a dereference protocol against an external third-party LIS infrastructure.



The TCS solution can exist in a number of routing states, depending on the transitional maturity of an overall NG9-1-1 system. For example, the company's [12a] IP-based ESRP can deliver calls to legacy PSAPs and NG9-1-1 PSAPs. All that changes is the type of equipment (routers, switches, and gateways) that needs to be installed at each location, and whether the CPE can accept SIP or if SIP signaling is being converted to analog.

[12a]

In the event the call taker is still using a legacy system, the call is converted back into analog format at the PSAP.

7.2.3.1. Availability – [RFP 6.2.3.1]

The LNG(s) shall be deployed in a manner that affords a minimum of 5-9's of availability. Provision should be made for a least two geographically diverse sites for hosting the LNG element(s).

The proposed solution is a NENA i3-compliant platform committed to the “five nines” standard (99.999 percent reliability) for providing the delivery and receipt of 9-1-1 calls. The proposed solution minimizes single points of failure; it is composed of redundant central system components that provide load sharing and load balancing with failover capability.

[12a]

7.2.3.2. SIP Conversion – [RFP 6.2.3.2]

The LNG shall convert all incoming 9-1-1 calls to SIP calls in accordance with the SIP requirements of NENA 08-003. Any BIDDER specific variations (optional parameters) and/or non-compliance from NENA 08-003 (including relevant SIP RFCs) must be identified and made available to MIL for distribution to potential PSAP CPE vendors.

[12a]

The PIF is fully compliant with RFC 3261 and also complies with the unique 9-1-1 signaling requirements through the use of [12a] trunk termination. Other versions of the PIF can support both multifrequency (MF) and enhanced multifrequency (E-MF) trunk termination and can convert to SIP as well. [12a]

[12a]. It is therefore imperative that any LNG/PIF be capable of understanding and interoperating with the signaling from the legacy SR to provide true bidirectional communications as needed (e.g., to support a tandem transfer to some other PSAP). The PIF also interworks the voice media received on the TDM side to RTP-formatted voice media for delivery within the proposed ESInet. In all cases for voice, the PIF will minimally employ a voice CODEC [12a]

7.2.3.3. Audio CODEC – [RFP 6.2.3.3]

All calls shall be encoded using the G.711 CODEC unless the incoming signaling includes the actual CODEC used to originally encode the call. If this information is available, the same CODEC will be used in the conversion of the call to a SIP call, provided that the destination PSAP supports that CODEC.

While not exhaustive, it is expected that the use of the following additional CODECs may be encountered:

- G.729
- AMR
- AMR-WB
- EVRC



- EVRC-B
- EVRC-WB
- EVRC-NW

BIDDERS shall describe all other (i.e., in addition to G.711) CODECs supported by the proposed system.

The TCS [12a] system will accept all listed CODECs. However, we believe best practice is to transcode any lower quality CODEC [12a].

7.2.3.4. LNG Call Recording – [RFP 6.2.3.4]

The LNG(s) shall provide functionality which maintains a log of all 9-1-1 calls received and processed by the LNG(s). Each call record within the log shall contain, at a minimum:

- Date & time of call: MM/DD/YYYY hh.mm.ss.s PTZ
 - o Start
 - o End
- ANI of call
- CPN of call (if different than ANI)
- Carrier for Call
- Call Type (i.e., Wireline, Wireless, VoIP)
- MOS
- Status (successful, busy, reorder, ring no answer, etc.)

The log(s) shall maintain at least seven (7) days of calls before being overwritten/purged or however maintained by the LNG functionality. It is left to the BIDDERS discretion as to whether hourly, daily or weekly files are created, but all log files shall be capable of being extracted in real-time i.e., do not have to wait until the file is complete and/or closed.

The format of the log files must be character-separated text (csv) text, suitable for simple importing to spreadsheet or word processing programs such as OpenOffice, Excel, Word etc.

We record logs for every call that enters our system. These logs contain a large number of reportable fields, and those fields are used to correlate events and capture Call Detail Records (CDRs). CDRs are stored on central servers, and we will maintain that data as per the requirements listed in this RFP. We will format the CDRs to capture the fields requested above.

7.2.3.5. LNG Call Reporting – [RFP 6.2.3.5]

Log files generated in accordance with 6.2.3.4 shall be extracted upon a monthly basis and sent via email to e911technicalservices@mil.wa.gov. Some emergency situations may require a real-time extract and BIDDERS should respond with how this will be achieved (e.g., contact and phone call, self-service automated system, etc.) and any limitations as to the frequency or timing of the extracts.

All call transactions are reported upon through our [12a]. We will generate the required monthly logs and deliver them via email to the address specified. In an emergency situation that requires a real-time extract, the Agency or other stakeholder should [12a] NOC, which will then escalate the request to a system administrator to capture the required information. We maintain a 24x7 on-call rotation so that a system administrator is always available.

There are no specific limitations as to the frequency of such requests, but we would not expect escalations to be necessary often, likely only on the order of one occurrence per quarter or less. If the frequency of requests is great enough, we will look to implement a self-service system to retrieve this information.



7.2.3.6. LNG/LIF Location Determination – [RFP 6.2.3.6]

The LIF shall provide the capability to obtain location information in order to create, populate and send (in subsequent SIP signaling) the PIDF-LO parameter as identified within NENA 08-003. The NLIS shall be queried to determine location information sufficient to define and populated a PIDF-LO. This PIDF-LO will then be passed to the ESRP (or terminating PSAP if BIDDERS provides this function as part of the ESRP implementation) in the SIP INVITE and used in determining the destination PSAP for the call.

If the LIF function is provided within the ESRP, it is acceptable for the LNGs to send a "location by reference".

Note: BIDDERS electing to provide this functionality within the ESRP shall indicate "Provided within ESRP" in the Exceptions, and select either the "Compliant" or "Compliant with Exceptions" Checkbox as appropriate to the proposed solution.

TCS [12a] ESInet LNG subsystem includes the NIF/LIF elements which perform the functionality as described (create a HTTP-Enabled Location Delivery [HELD] Dereference LbyV content identifier and add a PIDF-LO MIME body to the ESRP INVITE) for wireline and VoIP i2 (static) calls as recommended by the NENA i3 specification.

For wireless calls, the LNG NIF/LIF may query the NLIS if configured, but it always creates a HELD Dereference LbyR URI to include in the INVITE sent to the ESRP. INVITEs which arrive at the ESRP with a HELD Dereference LbyR URI and configured to route on location are dereferenced by the LNG LIF when the ESRP queries for location for "emergency routing."

In addition to the location servers listed for the NLIS (ALI, LIS, LDB) the NIF/LIF component can be configured to query what TCS refers to as an xPC, which is one of the various positioning center types: VPC, MPC, or a Gateway Mobile Location Center (GMLC) via the J-STD-036 and NENA 05-001 E2+ interface.

The LNG subsystem includes the flexibility to provision location retrieval from an NLIS element at an ANI/pANI, trunk, or system (ESInet) level.

7.2.4. BCF – [RFP 6.2.4]

The BCF provides a secure ingress into the ESInet for emergency calls presented to the network from either the Originating Network or from the PSAP. It incorporates firewall and admission control, and may include anchoring of sessions and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs or other entities connected to the ESInet.

The BCF may or may not include a Session Border Control (SBC) function at the BIDDERS discretion.

TCS will secure entry into the ESInet as required, on both the ingress and egress sides of the network, with redundant network appliances. The proposed solution includes [12a] at each PSAP for TCS remote support and connection to the ESInet.

[12a]

In an ESInet, the SBC applies control over SIP signaling and associated media to ensure that the call and call characteristics presented to the ESInet are predictable and acceptable. [12a]

TCS is a provider of both ESInet and IP-based call-routing and call-handling products. As described throughout this proposal, TCS products are 100 percent TCS engineered, built on open standards, and developed to meet NENA's published i3 standards. TCS' call-routing and call-handling technology can seamlessly integrate with other i3-compliant solutions through a direct SIP connection.



The proposed solution is interoperable with other NG9-1-1 systems on the market and is compatible with BCF/SBC vendors who meet the i3 requirements, such as [12a]

The SBC will support the following features that align with generally accepted security practices:

- Depending on the deployment model, the SBC either will act as a firewall or work cooperatively with an existing firewall.
- It will act as a transcoder for CODEC conversion.
- It will help resolve any topology issues that stem from either network address translation (NAT) deployment or bandwidth misalignments (e.g., preventing low-speed links from being oversubscribed with voice traffic).

With regard to SIP repair, the SBC will attempt to repair elements required to process the call on the ESInet; however, the lack of support for certain SIP elements will not be used as a means to deny a call (i.e., all calls will be accepted).

The SBC will have little or no impact on general call delivery and bandwidth performance characteristics, as it will be a high-performance, hardware-based component.

[12a]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

7.2.4.1. Availability – [RFP 6.2.4.1]

The BCF(s) shall be deployed in a manner that affords a minimum of 5-9's of availability. Provision should be made for a least two geographically diverse sites for hosting the Ingress BCF element and at least two geographically diverse sites for hosting the Egress BCF element.

The BCFs are deployed in a manner that affords a minimum of “five nines” availability. The ESInet is hosted [Redacted] [12a], which will also host the ingress and egress BCF elements.



7.2.4.2. SIP – [RFP 6.2.4.2]

The BCF (SBC) shall mediate all incoming 9-1-1 calls from VoIP providers to SIP calls in accordance with NENA 08-003. Any BIDDER specific variations (optional parameters) and/or non-compliance from NENA 08-003 must be identified and made available to MIL for distribution to potential PSAP vendors. It is not expected that calls arriving from the LNG element(s) will require the same level of mediation as they should already conform to NENA 08-003 SIP requirements.

The BCF, as noted, contains an SBC which will mediate incoming VoIP calls. We follow the NENA 08-003 guidance in our implementation of SBCs, both for direct SIP calls and converted TDM-to-SIP calls from the LNGs.

7.2.4.3. Audio CODEC Selection – [RFP 6.2.4.3]

All incoming VoIP calls should contain information as to the CODEC used to encode the call and the BCF (SBC) shall maintain the use of this CODEC for transport to the PSAP. If no CODEC information is available, the G.711 CODEC will be used.

[12a]
[Redacted]

7.2.4.4. Silence Suppression – [RFP 6.2.4.4]

If Silence Suppression is detected in the 9-1-1 call, the BCF (SBC) shall continue to use it for the duration of the call; otherwise Silence Suppression shall not be enabled.

[12a]
[Redacted]

7.2.4.5. Comfort Noise – [RFP 6.2.4.5]

If Silence Suppression is detected, optional functionality should be provided to insert “comfort noise”. This capability would be on a global basis, not a per-call or per-PSAP basis.

[12a]
[Redacted]

7.2.4.6. Text Support – [RFP 6.2.4.6]

The ESInet shall support Message Session Relay Protocol (MSRP) for relaying of text and IM messages to the destination PSAP.

The TCS solution will support Message Session Relay Protocol (MSRP).

7.2.4.7. Text Control Center (TCC) Integration – [RFP 6.2.4.7]

The ESInet shall have the capability to seamlessly receive Text-to-911 (SMS) messages from each carrier’s assigned TCC per Alliance for Telecommunications industry Solutions (ATIS) J-STD-110, Native SMS to 9-1-1 Requirements and Architecture Specification. Texts shall be processed within the ESInet according to the established ESRP/PRF routing rules.



Note: As Text-to-911 has only recently been implemented in Washington State and only at several PSAPs, our actual data is extremely limited. The preliminary data is indicating only 2-3 texts/day (average), but this could change once Text-to-911 is fully implemented statewide. The intent is for statewide Text-2-911 capability from day 1. Further, PSAPs currently receiving Text-to-911 messages receive them via a Web-based application (i.e., not over the ESInet). However, integrated receipt of Text-to-911 messages by the PSAP CPE is preferred.

The solution will comply with J-STD-110 [redacted] [12a]

[redacted] TCS is committed to providing software, equipment, and services that meet all applicable current and future NG9-1-1 standards within the timeline specified by NENA.

TCS adheres to i3 and related standards in the engineering of its solutions, including the IETF-defined protocol (RFC 3261) that describes a method for establishing multimedia sessions over the internet. RFC 3261 is used as the call-signaling protocol in VoIP, i2, and i3.

As can be seen in Exhibit 142, [redacted] [12a]

[redacted]. This means our NG9-1-1 solution interfaces with our own TCC directly, as well as with other TCC providers. Currently we route text according to the ESRP/PRF routing rules in the TCC, but we will provide the option of routing according to the NG9-1-1 ESRP/PRF in future releases, providing seamless alignment with existing routing rules.

[12a]



Exhibit 142. Texting Solution Overview



7.2.4.8. Video CODEC Support – [RFP 6.2.4.8]

At a minimum, all User Agents (UAs), if any, within the ESInet shall support H.264/MPEG-4 video. BIDDERS shall describe all other CODECs supported by the proposed system and describe how video will be implemented.

TCS will support H.264/MPEG-4 streaming video. Other video CODECs will be supported as standards bodies agree on implementation details. Currently, we recommend video to be implemented in a streaming fashion rather than as a static file.

7.2.4.9. BCF Session Recording – [RFP 6.2.4.9]

The BCF(s) shall provide functionality which maintains a log of all 9-1-1 sessions received and processed by the BCF(s). Each session record within the log shall contain, at a minimum:

- *Date & time of session: MM/DD/YYYY hh.mm.ss.s PTZ*
 - o *Start*
 - o *End*
- *ANI of session*
- *CPN of session (if available and different than ANI)*
- *Session Type (e.g., Wireline, Wireless, VoIP)*
- *Carrier for call (optional)*
- *Media (e.g., audio, text, video, etc.)*
- *MOS (originating and terminating)*
- *Status (successful, busy, reorder, ring no answer, etc.)*

The log(s) shall maintain seven (7) days of calls before being overwritten/purged or however maintained by the BCF functionality. It is left to the BIDDERS discretion as to whether hourly, daily or weekly files are created, but all log files shall be capable of being extracted in real-time i.e., do not have to wait until the file is complete and/or closed.

The format of the log files must be character-separated value (csv) text, suitable for simple importing to spreadsheet or word processing programs such as Open Office, Excel, Word etc.

Our BCF platform will record and report on the logs as specified, with the exception of media itself.

7.2.4.10. BCF Session Reporting – [RFP 6.2.4.10]

Log files generated in accordance with 6.2.4.9 of this section shall be extracted upon a monthly basis and sent via email to e911technicalservices@mil.wa.gov. Some emergency situations may require a real-time extract and BIDDERS should respond with how this will be achieved (e.g., contact and phone call, self-service automated system, etc.) and any limitations as to the frequency or timing of the extracts.

All call transactions are reported upon through our [12a]. We will generate the required monthly logs and deliver them via email to the address specified. In an emergency situation that requires a real-time extract, the Agency or other stakeholder should [12a] NOC, which will then escalate the request to a system administrator to capture the required information. We maintain a 24x7 on-call rotation so that a system administrator is always available.

There are no specific limitations as to the frequency of such requests, but we would not expect escalations to be necessary often, likely only on the order of one occurrence per quarter or less. If the frequency of requests is great enough, we will look to implement a self-service system to retrieve this information.



7.2.4.11. BCF (Terminating) to PSAP Connectivity – [RFP 6.2.4.11]

Each PSAP subtending the ESInet shall be connected via at least two (2) geographically diverse instances of BCF. BIDDERS shall make every attempt to provide true physical diversity to the PSAP, but MIL understands that this may not be possible for every PSAP within the state of Washington. For these instances BIDDERS must arrange for at least electrical diversity (e.g., separate VPNs, routers, etc.) to the PSAP CPE. BIDDERS shall identify which PSAPs cannot be provisioned with complete true physical diversity to the PSAP CPE and be willing to work with the PSAP, MIL and the various carriers and alternative transport providers/methods to develop/implement alternatives in order to achieve the desired level of diversity.

Attachment G provides the location information for PSAPs requiring connectivity.

All PSAPs are connected to our CLCs (and thus BCFs) through diverse MPLS networks. We believe our proposal provides true diversity to each PSAP, pending verification of last-mile circuits. True diversity is desired, but at a minimum we have provided for electrical diversity. We have requested and received diverse network quotes from our suppliers, but recognize that additional verification will be necessary to determine if any sites lack true diversity. We will identify the PSAPs where true diversity is not available in our solution and communicate that to the Agency for their consideration. We are happy to work with the Agency and the PSAPs to design the network with alternative transport methods where required.

7.2.5. ESRP – [RFP 6.2.5]

The ESRP is a critical function in the delivery of emergency service calls through the ESInet to the PSAP. BIDDERS shall provide a highly available and reliable ESRP function that meets or exceeds the 5-9's Availability criteria. While it is not anticipated that the state of Washington ESInet will require the deployment of Originating, Intermediate and Terminating ESRPs, it is left to the BIDDER to determine the most economical and efficient deployment of this element based upon the requirements contained within this RFP and the BIDDER's experience.

Within this RFP, the actual routing of calls is defined in the Policy Routing Function (PRF). At BIDDERS option, the PRF may be packaged as a subcomponent of the ESRP or the PRF may be deployed separately. If deployed separately, it also shall provide 5-9s Availability

The ESRP, or, at BIDDERS option, a separate but integrated SIP proxy function, shall be able to support administrative calls between call takers and PSAP administrators, and to destinations in the PSTN, as required to support situations that often arise in the handling of emergency calls and coordinating emergency responses to emergency situations. Examples of the uses of such administrative functions include adding a doctor or emergency room consultant to an emergency call involving a medical emergency, emergency call takers coordinating their response to an emergency situation, and PSAP administrators dealing with communication system outages in a geographic area.

The proposed [12a] ESRP/PRF is an i3-compliant ESRP soft switch employed to facilitate call routing on behalf of a calling endpoint, whether the endpoint is legacy or next generation (SIP). The ESRP and PRF are responsible for coordinating call routing via ECRF/LoST queries. [12a] is also responsible for policy implementation for NG9-1-1 applications and is the replacement for legacy SR technology. It includes a [12a] service that fulfills requests to map a call location.

7.2.5.1. General – [RFP 6.2.5.1]

The ESRP shall comply with the general requirements of Section 6.2.5 above.

[12a] complies with the general requirements in RFP Section 6.2.5.

7.2.5.2. ESRP Levels (NENA) – [RFP 6.2.5.2]

While it is not anticipated that the Washington State ESInet will require multi-level ESRPs (i.e., no "Intermediate ESRPs), BIDDERS proposals that incorporate them into the solution are not precluded. However, proposals that do incorporate Intermediate ESRPs must identify what benefits arise from such architecture. Further, should any ESRP



(regardless of level) be “shared” with anyone but MIL, BIDDERS must identify how the State of Washington is isolated from any other activity/usage as part of the response to 6.1.14.

TCS does not intend on using multi-level ESRPs within the state. As indicated, our response to RFP requirement 6.1.14 illustrates how the use of any shared components is managed to provide the highest level of availability within our solution.

If the Agency desires, we also can provide [12a] as a fully dedicated solution, as we’ve successfully done for other statewide customers. This option is more expensive, as each component of the system is entirely dedicated to the state of Washington, but it removes all “shared” components from the architecture (sans purely physical infrastructure such as shared power/cooling, generator backup, etc.). We have provided separate pricing for this option.

7.2.5.3. Dereferencing – [RFP 6.2.5.3]

For emergency service calls arriving with a SIP GeoLocation header containing other than a cid:URI parameter (implying location-by-value), the ESRP shall dereference the URI in an attempt to obtain the call’s location data. Alternatively, this process may be a part of the PRF.

The proposed [12a] LNG provides LbyV, populating the PIDF-LO within the SIP messaging with the full location of the caller via interaction with whatever legacy ALI DBMS infrastructure may exist or be implemented. This interaction complies with the NENA i3 standard. Also, [12a] will be capable of submitting queries to a NENA i3-compliant external LIS and to the required BCF to secure such interconnectivity and subsequent messaging. Furthermore, [12a] can provide location using a dereference protocol against an external third-party LIS infrastructure.

7.2.5.4. HELD – [RFP 6.2.5.4]

The ESRP shall implement a HTTP Enabled Location Determination (HELD) interface for dereferencing location-by-reference SIP location messages, or this capability shall be provided in the PRF.

[12a] is pre-engineered to support [12a] for the processing of 9-1-1 calls originating from both legacy and IP-based networks. [12a] will support the HELD dereference queries from i3 PSAPs.

During transition to NG9-1-1, the solution will support LbyR delivery for wireless calls and act as a proxy for subsequent HELD dereference queries received from an i3 PSAP destined for an ALI database. For wireline calls during transition, the TCS LNG/LSRG LIF will retrieve location from the ALI database and deliver location through the NIF in the form [12a] signaling to the i3 PSAP. The TCS solution is engineered to support the NLIS (with associated databases) for an eventual replacement of ALI. TCS’ documentation shows direct connections to the MPC, GMLC, and VPC that can be deployed when the state is ready to replace the ALI database entirely; while the ALI is in place, the TCS LNG/LSRG can query the ALI for the required data to support wireline, wireless, and VoIP calls without direct connections to the MPC, GMLC, and VPC.

7.2.5.5. TCP – [RFP 6.2.5.5]

The ESRP shall support TCP for the transport of SIP and HELD messages.

[12a] supports Transmission Control Protocol (TCP) for the transport of SIP and HELD messages.



7.2.5.6. Routing Policies – [RFP 6.2.5.6]

The ESRP shall support the invocation of distinct routing policies based on the incoming call queue, incoming URI, or IP address of the call source and/or or media type contained within the call. BIDDERS shall indicate and document all policies supported within their proposed solution.

TCS provides an ESRP/PRF to supply final policies before completing the call. In compliance with NENA standards and subject to Washington’s approval, our NG9-1-1 system will assign alternate and overflow routing policies via the PRF and offer the PSAPs [12a] with the ability to define and set each PSAP’s state. These policies will be fully documented and provided as part of the as-built documentation.

7.2.5.7. Sessions Originating from PSAP – [RFP 6.2.5.7]

It is highly desirable that the ESRP, in conjunction with PSTN and/or Internet Gateways, be capable of supporting seamless calling, conferences, transfers, and other typical Private Branch Exchange (PBX)-like functionality for calls terminating to (i.e., 9-1-1 calls) and 9-1-1 related calls originating from the PSAPs. For example, it must be possible to conference in language translation services (reached via an 800 number) onto an emergency (911 dialed) call in progress, or for an answering position to initiate a PSTN call to an automotive towing service provider via the ESInet. At a minimum, the SIP REFER method must be supported for i3 compatible PSAPs. Legacy CAMA PSAPs will still initiate transfers to other PSAPs by way of “Star Codes”, see 6.2.18.4, and are limited to only initiating transfers to other PSAPs.

TCS’ [12a] ESInet supports seamless calling, conferences, transfers, and other typical PBX-like functionality for terminating calls using the SIP REFER message, and it may be configured to accept and route PSAP administration line calls to the PSTN for eventualities such as tow service.

[12a]
[Redacted text block]

The [12a] LPG and RFAI NIF interfaces do not limit the conference or transfer to targets to only star or hash codes. [12a]

For PSTN calls initiated from the PSAP’s administration telephone line outside of a 9-1-1 call, routes can be set up from these lines over the [12a] ESInet (MPLS network) to the LSRG/LNG PIF (i.e., the media gateway) and out via SIP or TDM circuits to the Public Switched Telephone Network (PSTN).

7.2.5.8. Separate SIP Proxy – [RFP 6.2.5.8]

BIDDERS, at their discretion, may satisfy the requirements of 6.2.5.7 by providing an additional SIP proxy server(s) within the ESInet. However, it must be able to interwork with the ESRP to provide emergency call takers with a seamless experience accessing on-net and PSTN telephones. Further, if an additional SIP Proxy is provided, it must be deployed such that the ESRP AND the alternative proxy(s) achieve 5-9’s Availability. BIDDER shall also provide supporting information indicating how the 5-9’s is achieved.

As described in the response to RFP Section 6.2.5.7, the same SIP proxy and media gateway (LSRG/LNG PIF) used by the [12a] ESInet applications and subject to “five nines” SLA



will be used to provide emergency call takers with a seamless experience when accessing (conferencing, transferring, and PSTN calling) on-net and PSTN telephones.

7.2.5.9. Capacity – [RFP 6.2.5.9]

While the current ESInet is capable of accepting almost 3000 simultaneous calls, only ~600 can be completed due to the maximum number of call taking positions within the PSAPs. Accordingly, the BIDDER shall provide sufficient call processing capacity to initially accommodate up to 600 simultaneous 9-1-1 calls. If the BIDDER's solution is also rate limited, BIDDER shall state the maximum number of calls per second that the proposed ESRP solution can sustain for at least one (1) minute under "all up" conditions. Further BIDDER's response should also specifically address how text and multimedia calls will impact call handling capacity.

BIDDER's response should also address how additional capacity can be added and the costs associated with increasing capacity.

[12a] is designed to accept the maximum number of trunks available in the state, [12a]. However, in our view it is not plausible that all [12a] trunks would be carrying simultaneous calls, and designing the system to do so is economically prohibitive. We propose to accept the required [12a] trunks into the system so that any combination of the [12a] circuits can be in use at any given time. However, we do not expect all [12a] simultaneously be active, and as such we've designed the system for a lower rate [12a].

Currently, our solution is benchmarked [12a] with a call duration of at least one minute. This results in [12a] calls "in-flight" in the solution. Given that there would be a maximum of [12a] telecommunicators available, we will increase our capacity [12a]. We note that we have simply not had the request, prior to this RFP, to benchmark our system beyond the stated [12a], but we are currently investigating higher cps numbers that we would be happy to share with the Agency as tests progress.

If the Agency truly requires a [12a] rate we can accommodate the request, as our solution is highly scalable. Our solution is [12a] design that distributes calls across all available applications. Therefore, we can add more application processes to increase the cps rate, but the increase in cps bears an increase in cost as well. Once higher benchmark testing is completed we will be able to share those costs with the Agency.

7.2.5.10. Documentation – [RFP 6.2.5.10]

BIDDERS shall describe and list the features of the proposed ESRP, with particular emphasis on how it meets the general requirements of this section and the specific requirements herein. In particular, BIDDERS shall discuss how 5-9's is achieved and how the ESRP scales.

Features and Scalability

Because [12a] ESRP was engineered for use with widely available hardware, our solution has the greatest capacity for expansion. To add call-routing capacity to a region's growing network, [12a] only requires the purchase of additional service capacity. This ease of expansion is in direct contrast to many of our competitors' solutions, which require the replacement of – or extensive upgrades to – major hardware or software elements to achieve similar results.

An overview of our solution's features is provided in Exhibit 143.



Exhibit 143. [12a] Features

Feature	[12a] ESInet Enhancement per NENA i3
Location information	Supports unlimited amount of LOCATION DATA delivered with the emergency call either by value or by reference. Supports additional data on an "as needed" basis.
Additional data	Enables four standard types of additional data interfaces beyond the standard location information [12a]
Location validation	Provides validation based on PSAP GIS data, keeping routing addresses synchronized with the mapping system.
Caller data	Capable of delivering baseline subscriber data for wireline and VoIP users (as with E9-1-1), and supports the ability to deliver an unlimited amount of additional subscriber data, such as medical records, family contact information, and multimedia content, even for wireless subscribers (all subject to subscriber authorization).
Routing	Supports actual location-based call routing. Today this location may be provided by legacy means [12a]
Flexible alternate routing	Enables "just in time" routing changes to alternate PSAPs based on policy rules and through real-time updates under the PSAP's control, such as changes to call-routing boundaries in the GIS data.
Call transfer	Supports one-button call transfers to an unlimited number of transfer destinations. It is much more cost-effective to support cross-state and nationwide transfers with IP networks.
Legacy interface	Supports CAMA or IP to the PSAP and ISUP or IP from the communications service providers (CSPs).
Multimedia	ESInet supports the routing and delivery of multimedia, including text, files, and video.
Network resiliency	Multipathed, meshed networks for core services with multiple reroute options when any path is unavailable.
Transport costs	Relies on low-latency, digital IP circuits and networks that are often not subject to mileage or inter-Local Access and Transport Area (LATA) charges.
Reporting	Allows for flexible report generation and real-time views of system operation.

"Five Nines" Availability

All TCS safety and security technology – including [12a] – is engineered to exceed the "five nines" (99.999 percent) standard of reliability, also known as telco-grade reliability. To provide the QA our customers require, the TCS solution eliminates all single points of failure. Any component can be removed from the system without negatively impacting overall system capacity and performance. This means that routine maintenance, software upgrades, and PSAP expansion can be performed with no system downtime and with no loss of emergency call-routing capability.

TCS designs its systems for continuous 9-1-1 transaction processing, and we achieve this performance capability along with the utmost reliability through the intelligent use of a highly redundant system architecture. We process more than 200,000 9-1-1 calls daily on a nationwide basis and are pleased to offer the state of Washington our highly available NG9-1-1 system that can operate 24x7 as a true production system. Our [12a] architecture has four main

² NENA documents, *NG9-1-1 Additional Data* and *Emergency Incident Data Document*.



elements for stratified redundancy, each of which is incorporated into the proposed NG9-1-1 solution:

- **Site redundancy.** Our data centers with secure, monitored access [12a] will provide the system applications and network monitoring service. Each data center is equipped with the same software and hardware, and each is configured to process the full load of call traffic and network monitoring for the state.
- **System redundancy.** We configure our systems for [12a] call processing. By designing each system node to distribute traffic in the [12a] manner, our CLCs effectively load-balance traffic. Engineering the systems in this way also ensures that no failover is required during a catastrophic event in any one location.
- **Network redundancy.** The state will receive system and network monitoring services that are supported [12a]. Similar diversity and redundancy influence all network build-out aspects.
- **Software component redundancy.** The TCS distributed agent architecture supports high availability through the use of redundant software components available to perform the same task, running across multiple servers in multiple locations. We incorporate component redundancy in the construction of our [12a] system, combined with both local and geographic redundancy for all production processes, [12a]



Exhibit 144 shows an example of this redundancy, in this case for the ECRF/LVF architecture. All call-processing components are likewise redundant.

[12a]

A large black rectangular redaction box covers the majority of the page content, obscuring the details of Exhibit 144.

Exhibit 144. ECRF and LVF Architecture

In summary, TCS implements local redundancy with separate entrance facilities, redundant local area network (LAN) links between functional elements, and redundant hardware and software components. TCS implements geographic redundancy by deploying geographically diverse data centers and by employing carrier diversity, where available, between the MPLS network that provides call and data delivery to PSAPs and the MPLS network that provides the network and system monitoring.



We address resiliency and redundancy in many ways, emphasizing great attention to detail in our design.

7.2.5.11. ESRP Session Recording – [RFP 6.2.5.11]

The ESRP(s) shall provide functionality which maintains a log of all 9-1-1 sessions received and processed by the ESRP(s). Each session record within the log shall contain:

- Date & time of call: MM/DD/YYYY hh.mm.ss.s PTZ
 - o Start
 - o End
- ANI of call
- CPN of call (if different than ANI)
- Carrier for call
- Media (e.g., audio, text, video, etc.)
- Status (successful, busy, reorder, ring no answer, etc.)

The log(s) shall maintain seven (7) days of sessions before being overwritten/purged or however maintained by the ESRP functionality. It is left to the BIDDERS discretion as to whether hourly, daily or weekly files are created, but all log files shall be capable of being extracted in real-time i.e., do not have to wait until the file is complete and/or closed.

The format of the log files must be Character-Separated Value (csv) text, suitable for simple importing to spreadsheet or word processing programs such as OpenOffice, Excel, Word etc.

Strictly speaking, our ESRP (as a discrete functional element within the i3 architecture) does not receive media directly. The ESRP is a route determination proxy that controls the call that is “anchored” at the network edge on our telco-grade switch. That said, speaking of the ESRP as a legacy SR replacement (that is, as [12a]), we will record and report on the logs as specified. We will rely on our partner, [12a], to centrally log and record media payloads in the ESInet (although, again, not at the ESRP itself). [12a]

7.2.5.12. ESRP Session Reporting – [RFP 6.2.5.12]

Log files generated in accordance with 6.2.5.11 shall be extracted upon a Monthly basis and sent via email to E911TechnicalServices@mil.wa.gov. Some emergency situations may require a real-time extract and BIDDERS should respond with how this will be achieved (e.g., contact and phone call, self-service automated system, etc.) and any limitations as to the frequency or timing of the extracts.

All call transactions are reported upon through our [12a]. We will extract the log files monthly and email them to the specified address. If an emergency situation arises, the TCS [12a] will be contacted with the request and our engineering team will assist in obtaining a real-time extract.

7.2.6. PRF [RFP 6.2.6]

7.2.6.1. Availability – [RFP 6.2.6.1]

The PRF is a critical function in the delivery of emergency calls via the ESInet. BIDDERS shall supply a PRF that provides at least 5-9’s Availability. The PRF may be provided as a component within the provided ESRP, or as a separate component (i.e., physical device).

TCS provides an ESRP/PRF to supply final policies before completing the call. In compliance with NENA standards and subject to Washington’s approval, our NG9-1-1 system, via the PRF,



will assign alternate and overflow routing policies as well as offer the PSAPs a [12a] portal with the capability to define and set their PSAP state.

7.2.6.2. PRF Routing – [RFP 6.2.6.2]

The PRF must support at least the following:

- Alternate routing per PSAP (such as PSAP busy or unreachable)
- Default routes (such as based on incoming gateway trunk ID, call source IP Address, ANI exchange code, or any such similar data)

TCS provides an ESRP/PRF to supply final policies before completing the call. In compliance with NENA standards and subject to Washington's approval, our NG9-1-1 system, via the PRF, will assign alternate and overflow routing policies as well as offer the PSAPs a [12a] portal with the capability to define and set their PSAP state.

7.2.6.3. Legacy (PSAP) Routing – [RFP 6.2.6.3]

The PRF shall support tabular routing per PSAP (i.e., legacy MSAG/ESN-based ANI/ESRK) for calls arriving without accurate location data.

The PRF supports tabular routing per PSAP as a fallback mechanism for calls that do not have LOCATION DATA.

7.2.6.4. Rule-Sets – [RFP 6.2.6.4]

The PRF shall implement policies in the form of rule-sets must support the use of some parameters as variables.

7.2.6.5. Variables – [RFP 6.2.6.5]

The PRF shall implement variables as described in NENA 08-003. The following variables are explicitly required in the initial deployment:

- Date/Time of day
- ECRF query results

BIDDER shall also support any additional variables once defined and accepted by NENA.

The PRF should also support the use of additional variables in rules that reference status values that are contained within the SIP NOTIFY messages. For example, when the event packages are added to the SIP Event Function, PRF code changes should not be required in order to reference event values within the new event package. In a similar fashion, PRF code changes should not be required to write rules that reference previously unknown SIP header values. This does not preclude a table of valid variable names or other mechanisms that validate rules.

This capability should be available no later than Q3 2019.

[12a]

. This feature is on the TCS development roadmap, but will not be completed in time for deployment.

7.2.6.6. Configurable Subscription – [RFP 6.2.6.6]

Ideally the PRF shall be configurable to subscribe to relevant system and destination events for those entities that register with the SIP event function. For example, this feature permits downstream ESRPs or PSAPs to inform the PRF of their status (see the nena-ElementState and nena-ServiceState event packages in NENA 08-003) so that the PRF may apply the appropriate rules to the situation. However, as this functionality is still somewhat in flux within NENA, BIDDER shall describe alternatives for the PSAP to notify the system of its state. "The current



methods supported are a [12a] “make busy” tablet application. This feature is on the roadmap and slated for release [12a].”

7.2.6.7. Session Routing – [RFP 6.2.6.7]

For 9-1-1 calls that are treated for normal routing based on incoming call queue, status variables, and policy rules, the PRF shall query the ECRF to determine the destination PSAP. The PRF shall have access to at least two (2) ECRFs (e.g., at a minimum, a primary and a backup (failover) ECRF).

The TCS solution has geographically redundant ECRFs that are themselves also locally redundant; therefore, the PRF has at least four ECRF processes available to query.

7.2.6.8. Final Session Routing – [RFP 6.2.6.8]

The PRF shall invoke the rule-set associated with the SIP URI returned by the ECRF for final call routing.

The TCS PRF invokes the rule-set associated with the SIP URI returned by the ECRF for final call routing.

7.2.6.9. Invalid Rules – [RFP 6.2.6.9]

The PRF shall be implemented in a manner that it will flag, but otherwise ignore, invalid rules in the rule-set, and must always take a default action should it encounter a rule-set without encountering any actionable rule, or fail to find a specified rule-set. That is, the PRF must always deliver a call to some PSAP somewhere. Default actions should be configurable, and generate SIP events and/or SNMP traps to alert monitoring systems.

The PRF provisioning rules have built-in checks to disallow invalid rules. For example, rules to prevent circular routing are inherent to the provisioning interface. All call-routing rules have last routing options available that will be invoked if the specified PSAP set is not available. These events will generate [12a] that will be gathered and analyzed by the TCS NOC staff.

7.2.6.10. Issue SIP NOTIFY – [RFP 6.2.6.10]

The PRF shall issue a SIP NOTIFY to the SIP Event Function should a “notify” rule be encountered. This capability should be available no later than Q3 2019.

TCS is aware of this feature as described in NENA STA-010.2 i3 Architecture, Section 5.2.1.6 – ESRP notify Event Package, but has not yet implemented this feature. This feature is on the TCS development roadmap, but will not be available prior to deployment.

7.2.6.11. Session Processing Capacity – [RFP 6.2.6.11]

If the PRF is a distinct process from the ESRP, the PRF shall be able to process calls at the same or higher rate than the ESRP call processing rate.

The PRF can process calls at the same or higher rate than the ESRP processing rate.

7.2.6.12. Documentation – [RFP 6.2.6.12]

BIDDERS shall list and describe the features of the proposed PRF, with particular emphasis on how the PRF can reliably deliver emergency calls even in the presence of logical problems in the rule-sets or failures in other parts of the NG-9-1-1 system, such as the failure of the SIP event Function. If the PRF is a distinct process from the ESRP, BIDDER shall explain how this process and the ESRP achieve the required 5-9’s Availability.

The proposed [12a] ESRP/PRF is an i3-compliant ESRP soft switch employed to facilitate call routing on behalf of a calling endpoint, whether the endpoint is legacy or next



generation (SIP). The ESRP and PRF are responsible for coordinating call routing via ECRF/LoST queries.

The ESRP/PRF has the responsibility to supply final policies before completing the call. In compliance with NENA standards and subject to the Agency’s approval, our NG9-1-1 system will assign alternate and overflow routing policies via the PRF and offer the PSAPs a [12a] with the capability to define and set each PSAP’s state. We can configure the PRF to close a PSAP for certain hours or days of the week, on holidays, or during any scheduled time period. The call-metering feature can be adjusted for reduced staffing, PSAP equipment malfunction, or any other event affecting PSAP availability.

The PRF web portal can be seen in Exhibit 145 below, with the Time of Day tab selected. Also supported via the portal are options for PSAP Alternates, Alternate Routing Plans, and PSAP Shutdown. Each of these tabs has built-in logic to prevent routing errors such as circular routing.

Home Time of Day Alternates Alternate Routing Plans Shutdown

Select one from the following available responders

Name	FCC M	Record Status	Access Type
responder1-market123		EXPORTED	Read/Write
ENP-SAP-POLIZ		UPDATED	Read/Write
Stove-Test-2		UPDATED	Read/Write
Stove-Test-21		EXPORTED	Read/Write
Stove-Test-25		EXPORTED	Read/Write

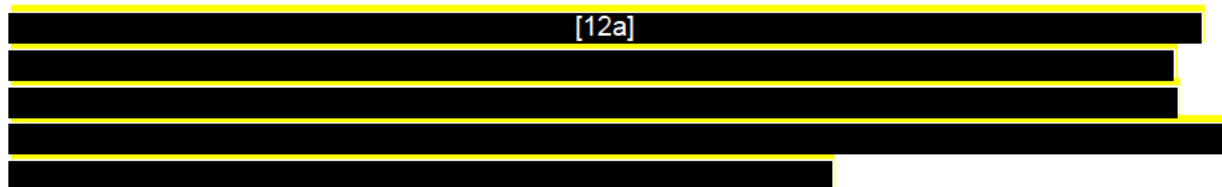
(Records: 1 - 5 of 7, Page: 1/2)

TOD Rules for Selected Responder

Responder Name	Rule ID	Start Date	End Date	Start Time	End Time	Effective Days	Export Status
responder1-market123	432	Fri 2015-06-26 00:00:00	Sat 2015-06-27 00:00:00	00:00:00	23:59:59	MO,WE	NEW
responder1-market123	433	Wed 2015-06-03 00:00:00	Fri 2015-06-26 00:00:00	00:00:00	23:59:59	TU	EXPORTED
responder1-market123	452	Tue 2015-06-23 00:00:00	Wed 2015-06-24 00:00:00	04:00:00	06:00:00	MO,WE	NEW
responder1-market123	542	Thu 2015-06-25 00:00:00	Sat 2015-06-27 00:00:00	00:00:00	23:59:59	TU	EXPORTED
responder1-market123	5243	Thu 2015-07-02 00:00:00	Sat 2015-07-18 00:00:00	00:00:00	23:59:59	WE	NEW

(Records: 1 - 5 of 6, Page: 1/2)

Exhibit 145. PRF Time of Day Example Rule



7.2.7. PRF Policy Rules Store [RFP 6.2.7]

7.2.7.1. Web Access – [RFP 6.2.7.1]

BIDDERS shall provide a web-based Policy Store portal that will permit authorized users to view the existing operational rule-sets, and, if the user has sufficient authority, to swap (exchange) specific rule-sets in the operational PRF Policy Store with alternate pre-validated rule-sets. All actions arising from the usage of this web-based portal shall be authenticated and logged per 6.2.19. The successful BIDDER shall document the pre-validated rule-sets prior to system migration. BIDDERS shall also explain the process for incorporating additional rule-sets into the PRF Policy Rules Store.

[12a] provides a [12a] portal for management of the PRF rules. Rules are validated to prevent routing errors, and after intent is confirmed the transaction is completed and logged. Example screenshots of these events are shown in the following exhibits.

Exhibit 146 shows a user adding a Time of Day rule.



Home Time Of Day Alternates Alternate Routing Plans Shutdown

Select one from the following available responders

Name	FCC ID	Record Status	Access Type
responder1-mohell 23		EXPORTED	Read-Write
EMF&AP-POUZ		UPDATED	Read-Write
Steve-Test-2		UPDATED	Read-Write
Steve-Test-21		EXPORTED	Read-Write
Steve-Test-25		EXPORTED	Read-Write

(Records: 1 - 5 of 7, Page: 1/2)

Add TOD Rule

Rule ID: 3245 Start Date: End Date:

Available Days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Effective Days: [Empty]

Start Time: 00:00:00 End Time: 23:59:59

Add Cancel

Exhibit 146. [12a] User Adds Time of Day Rule

Exhibit 147 shows a confirmation screen for the user.

Export

You are about to export a TOD Rule with Rule ID :422. Do you wish to continue with the export process?

Export Cancel

Exhibit 147. [12a] Confirmation Screen

Exhibit 148 shows a summary view of transaction logs. Note that additional details about a transaction are available, as shown in the first line of the History tab.

History

Modified By	Modified Date	Request Id	Responder Number	Rule Id	Effective Day
System	Tuesday, June 16, 2015 8:16:01 PM	1157	1	1115	WE,TU
Effective Start Date : Wednesday, June 10, 2015 6:00:00 AM				Effective End Date : Friday, June 19, 2015 5:00:00 AM	
Start Time : 010100				End Time : 030000	
System	Tuesday, June 16, 2015 11:37:40 PM	1207	1	1115	MO,TH,TU,WE
System	Thursday, June 18, 2015 7:46:54 PM	1511	1	1115	
System	Thursday, May 21, 2015 4:46:53 PM	214	1	12	MO
System	Thursday, May 21, 2015 4:47:54 PM	215	1	12	MO
System	Thursday, May 21, 2015 5:05:43 PM	216	1	12	MO
System	Thursday, May 21, 2015 5:06:58 PM	217	1	12	FR
System	Monday, June 15, 2015 5:23:30 PM	1023	1	12	FR
System	Monday, June 15, 2015 5:23:48 PM	1024	1	12	FR
System	Thursday, June 18, 2015 7:46:31 PM	1506	1	12	

(Records: 1 - 10 of 68, Page: 1/7)

Highlight Changes Close

Exhibit 148. [12a] Summary View of Transaction Logs

7.2.7.2. Rule-Set Changes – [RFP 6.2.7.2]

The Policy Store portal of 6.2.7.3 shall permit users with sufficient authority to submit rule-set additions, deletions, or changes. Such changes must undergo a validation process that includes automated syntax checking and functional review before they are accepted and made available as an alternate rule-set in the list of pre-validated rule-sets. The rule should also undergo a semantic validation process, such as examining the rules for the use of undefined-variables, the absence of a final default action, or the possibility of a circular reference between rule-sets.



Rule sets are validated before changes are made. If a rule set deletion, addition, or change creates a logical routing problem, [12a]. Our web portal assists the user in modifying or creating rules through the use of pre-populated views, as seen in Exhibit 149, which shows a new Time of Day rule being created.

The screenshot shows a web portal interface for creating a Time of Day rule. At the top, there are navigation links: Home, Time of Day, Alternates, Alternate Routing Plans, and Shutdown. Below this is a table titled 'Select one from the following available responders'. The table has columns for Name, FCC ID, Record Status, and Access Type. The first row is highlighted in blue and contains the following data: Name: Respondent-monet1 23, FCC ID: ENFDAP-FOLZ, Record Status: EXPORTED, Access Type: Read-Write. Other rows include 'Sleve-Test 2', 'Sleve-Test 21', and 'Sleve-Test 25', all with Record Status: EXPORTED and Access Type: Read-Write. Below the table is a pagination control showing '1 2' and a record count '(Records: 1 - 5 of 7, Page: 1/2)'. Below the table is a section titled 'Add TOD Rule'. It contains a form with 'Rule ID: 3245', 'Start Date:' and 'End Date:' fields. Below this is a calendar interface with 'Available Days' and 'Effective Days' columns. The 'Available Days' column lists Monday through Sunday. Below the calendar are 'Start Time: 00:00:00' and 'End Time: 23:59:59' fields. At the bottom right of the form are 'Add' and 'Cancel' buttons.

Exhibit 149. New Time of Day Rule Being Created on [12a]

7.2.7.3. Portal Access – [RFP 6.2.7.3]

The web portal to the policy store shall be configured to allow access from a secure (e.g., two-factor authentication) remote VPN appliance also located within the PSAP premises.

Access to the web portal is subject to authentication of the user as well as network controls. The portal is accessed from within our closed network using port and pinhole firewalling. These controls ensure traffic is allowed only through certain ports that are opened in the firewall.

7.2.7.4. Logging – [RFP 6.2.7.4]

The Policy Store system shall maintain a log of all changes made to the Policy Store, including the identification of the party making the changes.

As seen on the History screenshot in Exhibit 148, the policy store maintains a log of all changes, including identification of who makes the change.

7.2.7.5. Backup – [RFP 6.2.7.5]

The system shall maintain at least two (2) backup copies of the Policy rules. The two (2) backup copies shall be located at geo-diverse sites.

The relational database tables that contain the policy rule-sets will be exported/backed up [12a]

7.2.7.6. Example Rule-Sets – [RFP 6.2.7.6]

BIDDERS shall submit several examples of the rule-sets utilized by their proposed solution, and clearly describe the process by which additional rule-sets can be submitted for addition to the production system.

Examples of rule-sets have been shown throughout Section 4.2.7, and an additional rule-set is shown in Exhibit 150. This rule-set shows how alternates are provisioned in the system. An available responder is selected, and the current routing information for that responder is shown.



Maintenance to the records is supported by pre-populated fields and built-in logic and syntax checking to assist the user in making changes. Additions to the rule-sets are managed via the portal or by contacting the TCS [12a] with requests for changes. The TCS [12a] is able to provision emergency changes (e.g., PSAP shutdown) on behalf of the PSAP, but rule management is otherwise encouraged through the portal or by requesting a change via our PM.

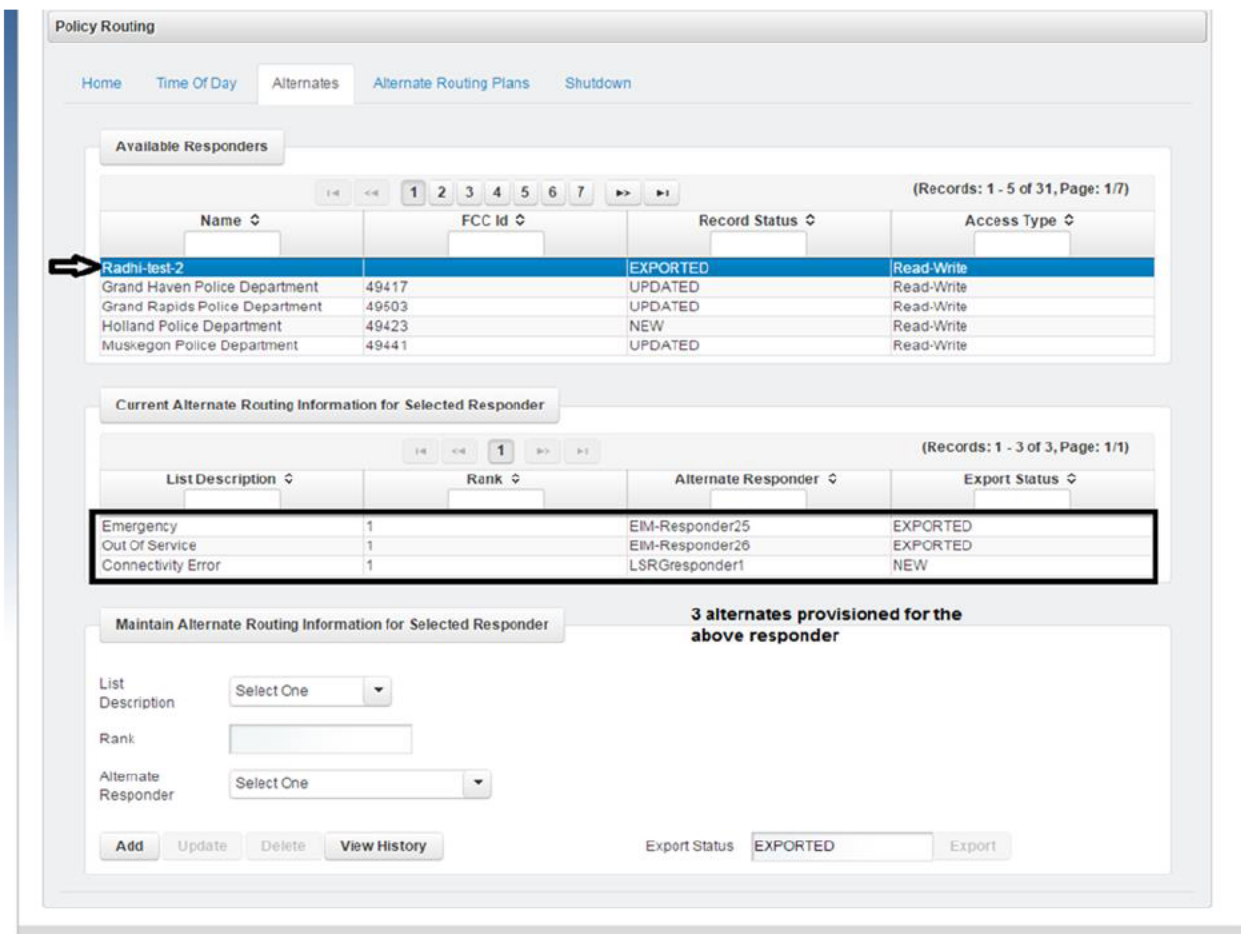


Exhibit 150. Policy Routing Function Portal

7.2.8. ECRF [RFP 6.2.8]

The BIDDER shall provide a clear description of the proposed ECRF, list its features and capabilities, discuss its error handling, default mechanisms and logging, and provide an overview of how it is deployed and achieves high reliability.

This section also includes some basic GIS requirements in order for the ECRF to perform its basic routing functions. BIDDERS responding with a complete and separate GIS solution are advised to also consider the requirements of Section 6.2.11. Regardless of how implemented, the GIS description must also discuss how the required interfaces will be preserved, the GIS update process, frequency and how information would be exchanged with MILs GIS services vendor, if different from the BIDDER, including the handling of error reports. BIDDER shall identify any exceptions or non-compliance issues that may arise from MIL's request for NLIS functionality.

TCS has included its [12a] ECRF as a geospatial routing platform built to conform to a NENA i3-defined ECRF. Our solution consists of the following functional components:

- GIS database



- ECRF business logic
- Hypertext Transfer Protocol Secure (HTTPS) server

The ECRF can accept, among other layers, polygons, line segments, and address points from Washington's GIS. Attributes provided must meet the minimum [12a] ECRF specifications, which we will determine with input from Washington's GIS personnel.

[12a]

It offers a wide array of call-routing options based on all of the perceived shapes that could represent the location of the 9-1-1 caller. These include:

- [12a]
- [12a]
- [12a]
- [12a]

In addition, the ECRF is capable of handling many service boundaries that represent the downstream ESInet/PSAP boundaries. It is capable of the following output responses:

- FindService
- GetServiceBoundary
- ListServicesByLocation

Washington's GIS data will be loaded onto each ECRF server as part of the equipment staging process. Connectivity to [12a] of the GIS master database eliminates the prospect of a single point of failure.

We will be responsible for all GIS database management related to the [12a] ECRF, including:

- Replicating the master GIS database and maintaining interconnection with the ECRF databases.
- Correcting GIS data inconsistencies, errors, or anomalies for data reconciliation.
- Researching issues related to the GIS data layers, as necessary, and applying any required configuration changes.
- Providing QA and "publishing" any routing data received from the single master GIS database before automatically updating production routing databases.
- Monitoring database availability and health, replication topology, and maintenance plans, as well as providing upkeep of database maintenance plans, database schema, and replication topology.
- Managing all configuration questions and changes, including, without limitation, production spatial routing changes and GIS database updates.

[12a] ECRF has built-in audits and error handling that will notify Washington's systems administrators via [12a] when data received from the single GIS master database does not



meet conformity requirements. Washington and [12a] will work directly with the appropriate 9-1-1 entities to make any necessary updates to GIS data. Washington will then resynchronize updated GIS data to the TCS “auditing” geodatabase via the [12a] SIF. If data has not passed audit, the workflow described above must be repeated until such data issues have been remedied by the state.

[12a]

The [12a] ECRF server includes the following features:

- Compliance with IETF LoST standards
- Ability to provide routing information for NG9-1-1 call location
- Ability to identify the correct PSAP from GIS map layers ([12a]) so that the call can be routed to the appropriate ESA
- Validation of civic and geodetic locations
- Secure client authentication
- Redundant web services
- Request for service results returned in milliseconds
- Multiprocessor and multithreaded support
- Cached queries
- Load balancing supported
- Queries supported: [12a]
- Support for [12a] and file geodatabases
- Runs on COTS equipment
- Support for errors, warnings, and redirects

7.2.8.1. ECRF NENA – [RFP 6.2.8.1]

The BIDDER shall provide the NG9-1-1 ECRF as defined in the NENA 08-003 Detailed Functional and Interface Standards for the NENA i3 Solution.

[12a] ECRF is a software-based application that provides the functionality required of an ECRF for location based routing, per NENA 08-003.

7.2.8.2. Availability – [RFP 6.2.8.2]

The ECRF is a critical function in the delivery of emergency calls via the NG9-1-1 Routing Service. The BIDDER shall supply an ECRF function at a minimum of two (2) geographically diverse sites that provides at least 5-9's of Availability.



We have designed our network for “five nines” service, allowing for no single point of failure in the equipment or network itself. The data centers supporting the ESInet are geographically diverse sites [12a]

7.2.8.3. ECRF Interface – [RFP 6.2.8.3]

The ECRF must interface and provide location-based emergency call routing functionality via the RFC 5222 (LoST protocol) and the functional specification of NENA 08-003.

[12a] ECRF is a [12a] LoST service that fulfills requests to map a call location. It provides the query mechanism for agencies to identify the correct ESN from GIS map layers in order for calls to be routed to the appropriate emergency service. The underlying service application is involved in geocoding an address and returning location information. Spatial queries use geospatial (x-y) or civic (street address) location information to determine which PSAP should receive a particular call.

These [12a] ECRF services perform a number of requests centered on mapping locations and service Uniform Resource Names (URNs) to service URIs. The [12a] ECRF server identifies the proper ESN from GIS map layers so calls can be routed to the appropriate emergency service agency (ESA).

The [12a] ECRF server is an industry-tested platform that complies with all required functionality as described in NENA i3 documentation pertaining to both LVF and ECRF.

The [12a] ECRF is capable of receiving a SIP URN (specific to 9-1-1) and a PIDF-LO and returning a SIP URI, which is indicative of the “next hop” proxy or destination to which a 9-1-1 call must proceed. In order to complete the call-routing process, the transaction is supported through the use of IETF LoST protocol (RFC 5222).

An [12a] ECRF server is always deployed in a redundant, highly available configuration. Generally, each data center in an ESInet would host an [12a] ECRF server and its associated services. The configuration consists of redundant central system components that provide load sharing with complete failover capability. The proposed technology is built to meet or exceed 99.999 percent reliability. The redundant database architecture allows multiple switches to provide load sharing with multiple [12a] Server databases. With load sharing, the system will continue to run seamlessly, even if a database is taken offline.

Depending on available GIS data, the ECRF also can support sub-SOS-level lookups for police, fire, and EMS destinations, as well as a variety of other services (e.g., water department, power company). If provisioned, various SOS-designated emergency services can be included for additional granularity.

The [12a] ECRF server includes the following features:

- Compliance with IETF LoST standards
- Ability to provide routing information for NG9-1-1 call location
- Ability to identify the correct PSAP from GIS map layers ([12a]) so that the call can be routed to the appropriate ESA
- Validation of civic and geodetic locations



- Use of location values or references
- Secure client authentication
- Unlimited role-based queries
- Redundant web services that support queries from any platform
- Request for service results returned in milliseconds
- Multiprocessor and multithreaded support
- Cached queries
- Load balancing supported
- Queries supported: [REDACTED] [12a]
- Recursion and iteration with other LoST servers on the ESInet
- Support for [REDACTED] [12a] and file geodatabases
- Service boundaries returned by value or by reference
- Runs on COTS equipment
- Support for errors, warnings, and redirects
- Supports location references or values

With the spatial routing of calls, the [REDACTED] [12a] ECRF server enables calls to be routed based upon their geographic location to a prescribed PSAP by routing on a point-in-polygon lookup, not just ESN. Furthermore, other rules can be defined in [REDACTED] [12a], such as call delivery based upon the geography of an incoming call.

[REDACTED] [12a] supports the following:

- LbyV: a typical PIDF-LO/ALI record [REDACTED] [12a]
- LbyR: a unique ID that signifies the location/record that should be retrieved to obtain location information [REDACTED] [12a] (typically this is retrieved from a carried-based LIS)
- Traditional ALI lookup: ANI used to receive ALI
- ALI steering: [REDACTED] [12a]

7.2.8.4. ECRF Access – [RFP 6.2.8.4]

The ECRF shall support LoST queries (via Transmission Control Protocol [TCP]) from ESRP(s), PSAP customer premise equipment (CPE), or any other permitted IP host within MIL's ESInet. The ECRF may rate-limit queries from sources other than provisioned ESRPs.



The TCS [12a] is designed to handle LoST queries from all provisioned ESRPs, CPE, and other permitted IP hosts. In practice, we have [12a]

7.2.8.5. ECRF Logging – [RFP 6.2.8.5]

The ECRF shall log all connections, connection attempts, and LoST transactions.

[12a] logs connections, connection attempts, and LoST transactions.

7.2.8.6. GIS Routing Database (Function) – [RFP 6.2.8.6]

Unfortunately, NENA 08-003 has made several assumptions that may not hold for Washington State, in describing the “end state” of the i3-based ESInet that MIL is seeking. In particular, assumptions 4 and 5 (of Executive Overview) where, respectively, some PSAPs are likely to still be CAMA-based and require ALI/MSAG functionality and there may be no “GIS system” which automatically propagates changes to the ECRF and LVF.

Accordingly, MIL is requesting that the BIDDER provides a stand-alone GIS function (in event of no Statewide GIS database) and associated underlying data that allows the ECRF (and LVF if applicable) to determine the correct PSAP to route the call to. BIDDERS shall inform MIL of any data or data-sets that are required from MIL to realize this function. BIDDERS shall provide a detailed description of the solution.

Once a statewide GIS database (i.e., the “9-1-1 Authority’s GIS System” assumed by NENA) becomes available it is required that the ECRF (at a minimum) support the following requirements. It is understood that some functionality may be initially unavailable/unnecessary depending on BIDDERS proposed solution. BIDDER shall clearly identify these cases and identify any limitations in the interim period.

With a dedicated, experienced project team, [12a] will provide the state of Washington with an initial NG9-1-1 stand-alone GIS dataset for routing calls, based on existing data available within the state and from county 9-1-1 authorities. This will include mechanisms for continuously updating the dataset to produce seamless, statewide coverage. [12a]’s solution includes a variety of core components for acquiring location GIS data updates, performing GIS data transformation and GIS data normalization, executing automated QA/QC checks, reporting discrepancies back to counties, and providing a seamless statewide GIS dataset.

At a high level, [12a]’s NG9-1-1 GIS managed services solution includes the following elements:

- Subscription-based access to [12a]’s enterprise GIS data management tools:
 - [12a] Server GIS Portal for easily transferring GIS data and viewing GIS update status
 - [12a] Discrepancy Viewer to efficiently communicate GIS data errors to counties and regional authorities for resolution
- GIS implementation services to organize GIS data sources for the system, develop the QC plan, and identify key roles in the NG9-1-1 GIS data workflow process
- NG9-1-1 GIS Managed Services, which provide ongoing GIS data transformation, aggregation, QA/QC, and reporting

Throughout this project, [12a] will dedicate time to project management and ongoing communication. [12a] will provide regular status updates, including:

- General progress updates



- Meetings held, planned, or needed
- Issues/problems encountered or anticipated
- Goals for the next reporting period
- Schedule review
- Customer responsibilities

[12a] will schedule an on-site project initiation meeting with key project stakeholders to present the project approach and the anticipated project schedule. The initiation meeting will be held at a centrally located meeting space. The agenda also will include reviewing project objectives and goals, defining mutual expectations, and establishing communication processes.

[12a] understands that all communication needs to be coordinated via the vendor and Washington. [12a] understands that all communication needs to be coordinated via the vendor and Washington.

[12a] will create an initial statewide GIS dataset for NG9-1-1 by combining GIS data layers from the state and local entities, including all of the county 9-1-1 authorities. Local GIS data may be submitted to [12a] by individual counties or regional authorities via one of the following methods:

- [12a]

This initial GIS dataset will be statewide in that it will incorporate existing data throughout the state. In order to route calls to the correct dispatch center using this GIS data in the proposed ECRF, and subsequently forward them to the appropriate responder, the following minimum GIS layers will be required throughout the state:

- Street/road centerline, with road ranges
- PSAP boundary
- County boundary
- Emergency service boundaries

If not available from the state, individual counties, or regional authorities, [12a] can populate the street/road centerline and county boundary layers based upon publicly available sources (such as [12a]). If not available, [12a] can develop PSAP and/or emergency services zone (ESZ) boundaries or synchronize the road centerline layer to the MSAG for individual counties at an additional cost and under a separate CONTRACT between the individual county and [12a].

The optional layers outlined in RFP Section 6.2.11.3 also can be integrated into the GIS dataset, [12a]

Note: While [12a] will provide ongoing QA/QC audits and the data updates that fail QC checks will not be provisioned into the ECRF, the quality of the data included in the statewide dataset is ultimately the responsibility of individual counties.



To facilitate the creation of a uniform statewide GIS base map, automated schema and geodetic transformation procedures will be executed to assimilate the source GIS data layers into the authoritative GIS data model. If available, the individual GIS data layers referenced in RFP Section 6.2.11.3 will then be merged into a statewide dataset.

The proposed system accommodates differing data models and geodetic systems from disparate 9-1-1 GIS data sources. Counties will be able to continue working with their existing data structure, if needed, and still have updates incorporated into the statewide dataset.

[12a] will implement a QA/QC process to ensure data meets the state of Washington's NG9-1-1 criteria; this process will automatically report GIS errors to the authoritative 9-1-1 source (as described in Section 6.2.11) for correction. In order to create topological accuracy across county boundaries, [12a] also will create reference layers along county boundaries to which local authorities can match points and polygons. As counties, regional authorities, and/or the state improve their data based on these error reports and reference layers, the GIS dataset will become increasingly more complete and seamless. As described in RFP Section 6.2.11.8, [12a] also will produce quarterly audits of each county's data in comparison to its MSAG and ALI database.

After layers are aggregated together, the GIS dataset will be loaded into the [12a]

[12a] As part of this process, [12a] will:

- Create, configure, and load [12a] locators for simple address lookups
- Design [12a] map documents [12a] for [12a] (layers, layer order, layer visibility, scale dependent display, symbology, labeling, etc.) based on project stakeholders' preferences
- Develop, configure, test, and publish [12a] map services

This will result in a stand-alone GIS function that can provision to the ECRF and LVF to allow it to route incoming calls to the correct PSAP, as well as provide the framework for developing a single, seamless statewide GIS dataset.

7.2.8.6.1. GIS Compliance – [RFP 6.2.8.6.1]

The ECRF shall comply with GIS standards including, but not limited to, NENA Standard for NG9-1-1 GIS Data Model (draft) and NENA 02-010V9 and NENA 02-014v1. The ECRF complies with NENA standards, any draft standards will be compliant once approved (and time allowed for implementation)

[12a] actively participates on the NENA workgroup currently working on the NG9-1-1 GIS Data Model. [12a] is prevented from making particular business claims around the NG9-1-1 GIS Data Model Draft, not yet released for public review, by NENA-ADM-002.1, Section 4.1. [12a] believes it can still meet the spirit and intent of the requirement, but we understand the Agency may view this as an exception.

7.2.8.6.2. GIS Updates – [RFP 6.2.8.6.2]

The ECRF shall support updates to the GIS database without disruption of ECRF LoST service. BIDDERS shall explain how this is achieved.

The ECRF will allow updates to the GIS database without disruption of the LoST service. We manage ECRF updates so that no operational problems are created. We perform a QA check on



the GIS data when it is loaded into a staging database. We check for standard GIS errors, such as gaps/overlaps and conflicts, during this QA process prior to loading to the ECRF. We refer any errors found at this stage to [12a] for resolution. Therefore, only “clean” data is loaded into the ECRF through a database replication technique that does not cause operational issues.

7.2.8.6.3. Shape Files – [RFP 6.2.8.6.3]

In addition to ESRI file geodatabase and/or geodatabase, the ECRF GIS database shall also support updates via ESRI shapefiles.

The proposed [12a] GIS SIF database accepts shapefiles. The SIF will not use shapefiles for updating the ECRF/LVF GIS databases. Those updates will be automatically synchronized at regular intervals with the SIF database via either [12a] replication.

7.2.8.6.4. GIS Database Validation – [RFP 6.2.8.6.4]

The ECRF (or associated administrative program) shall be able to view and validate GIS database changes before they are applied, for example, detect overlaps or gaps in geographical boundaries contained in a layer.

The TCS [12a] ECRF GIS data flow process includes a GIS staging server for QA purposes. This would include, for instance, checking for gaps and overlaps before the GIS updates are presented to the ECRF.

7.2.8.6.5. Location Errors – [RFP 6.2.8.6.5]

All location information errors must be made available to the County 911 Coordinator and agency for resolution and geocoding errors will be written to a separate log or file, so that they may be easily handed off for investigation and correction.

TCS employs various GIS management tools to migrate existing datasets into the company’s schema. Data maintenance will initially be performed at the SIF product, which will generate geocoding errors. The QA process continues in the TCS GIS department prior to loading GIS data to the ECRF for the purpose of identifying any remaining errors.

7.2.8.6.6. Routing – [RFP 6.2.8.6.6]

At a minimum, the ECRF must be able to route locations based on geographical coordinates (LAT/LON) or based on civic addresses (house #, street, city, etc.).

[12a] ECRF can route locations based on geographical coordinates or civic addresses.

7.2.8.6.7. GIS Database Access – [RFP 6.2.8.6.7]

The BIDDER shall provide a Web portal that permits the County 911 authority secure (e.g., two-factor authentication) administrative read-only access and export capability to their records within the GIS database. This function may be rate-limited to avoid impacting emergency call delivery services.

The county 9-1-1 authority will have secure, administrative, read-only access and export capabilities for the records within the GIS database as a copy of the production data. [12a]

Instead, That is, to ensure the GIS data is kept as secure as possible, [12a] will have access to a read-only copy of the GIS database, but [12a] will provide the [12a] with exports of the production GIS database if needed.



7.2.8.7. ECRF Capacity – [RFP 6.2.8.7]

The BIDDER shall state the maximum number of queries per second the proposed ECRF can sustain for at least one minute under adverse but “all up” conditions. While exact number of queries per second is unknown at this time, BIDDERS should consider that the Originating Network is capable of presenting almost 3000 simultaneous calls to the ESInet, not including the impact of text messages.

[12a]

7.2.8.8. ECRF Documentation – [RFP 6.2.8.8]

The BIDDER shall provide documentation describing ECRF operation, maintenance and listing the features of the proposed ECRF, with particular emphasis on how it meets the specific requirements herein.

Following installation and system cutover, TCS always supplies full as-built documentation as part of the purchase. A complete description of the functional elements, including ECRF, will be available as part of the as-built documentation, and the ECRF features are included here for consideration.

The [12a] ECRF server includes the following features:

- Compliance with IETF LoST standards
- Ability to provide routing information for NG9-1-1 call location
- Ability to identify the correct PSAP from GIS map layers ([12a]) so that the call can be routed to the appropriate ESA
- Validation of civic and geodetic locations
- Secure client authentication
- Redundant web services
- Request for service results returned in milliseconds
- Multiprocessor and multithreaded support
- Cached queries
- Load balancing supported
- Queries supported: [12a]
- Support for [12a] and file geodatabases
- Runs on COTS equipment
- Support for errors, warnings, and redirects

A full documentation library exists for all subscribers to the solution, with individual guides for users, PSAP administrators, and system administrators. This documentation includes material that describes systems operations and procedures.



7.2.9. Location Validation Function (LVF) – [RFP 6.2.9]

The LVF is not a critical function involved in real-time emergency call delivery, but, once LISs are deployed in the Originating Network, it must be available to call origination providers and to the general public at large so these parties can verify that civic addresses or latitude/longitude will return PSAP or emergency responders URIs.

In view of MIL's requirements for a NLIS, it is left to the BIDDER's discretion as to whether an LVF should be 1) deployed in the initial architecture, or 2) deployed at a later stage in the evolution of the ESInet. (i.e., when LISs are deployed in the Originating Network itself.. Regardless of the case, BIDDERS must describe how civic address validation will be accomplished within the proposed solution.

If provided as part of the BIDDER's initial solution, BIDDER shall describe:

- NENA Compliance
- Availability
- Database synchronization (i.e., with ECRF)
- Interfaces Supported
- Web Portal
- Documentation

If provided at a future date, BIDDER must provide any cost impacts to proposed pricing; and the LVF will be required to comply with the then relevant NENA documentation.

TCS has included LVF in our proposal as an element [12a]

NENA Compliance

[12a] LVF is an IETF [12a] LoST server that provides the NENA i3 functional elements of LVF as specified in NENA TSD 08-003.

Availability

To ensure the proposed LVF remains highly available, [12a] LVF will be deployed in a fully redundant [12a] manner, in a [12a] at initial implementation. The [12a] LVF system will be provisioned using the same data as the [12a] ECRF, which will ensure the system is kept as available and current as possible. As designed, the LVF system is easily expandable, allowing for additional redundancy and capacity as the Agency requires by implementing additional hardware to the system.

Interfaces Supported

[12a] LVF supports the LoST interface.

Web Portals

[12a] Spatial Router is equipped with a dashboard for monitoring real-time statistics, load, query response behavior, and individual query contents, systemwide and per server.

Documentation

The [12a] Spatial Router LVF can be used directly by any authorized 9-1-1 entity needing to perform NG9-1-1 i3 location validation in place of or alongside legacy 9-1-1 MSAG-style validation. The [12a] Spatial Router supports LVF using site and/or structure layers and also addresses ranged road centerline layers.

In i3 networks, MSAG is replaced with a GIS-based LVF. Before civic address locations are entered or updated in a LIS, the address records must be validated to ensure they are adequate for routing and dispatch. This is accomplished by locating the civic address in the authoritative GIS database for the service area, as shown in Exhibit 151.

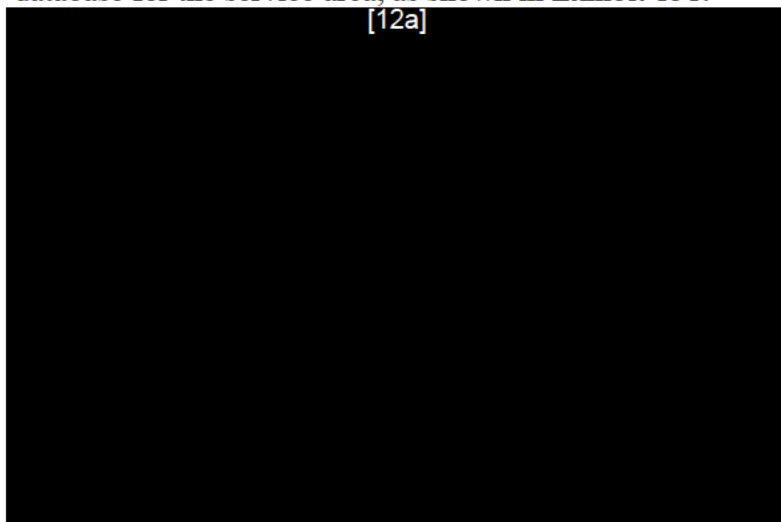


Exhibit 151 [12a] Spatial Router

[12a] When this attribute is present and set true in the query, the [12a] treats the request as a location validation request and returns a LoST [12a] that includes location validation elements stating which parts of the provided civic location passed validation, failed validation, or were unchecked. The same geospatial data set is provisioned to all [12a] in the system, whether they are being used for ECRF or LVF queries.

Features

- IETF [12a] LoST server providing NENA i3 LVF
- Validates civic locations prior to entry into a LIS using the LVF
- Can play multiple roles in LoST hierarchies, including Forest Guides, state level LVFs, and “leaf node” LVFs
- Supports PIDF-LO geodetic location types of point, polygon, circle, ellipse, and arc-band
- Supports PIDF-LO civic location types, including fine grained components handling building, floor, suite, room, and seat

Exhibit 152 shows a design schematic for the LVF.



[12a]

Exhibit 152. [12a] (LVF)

7.2.10. PSTN Gateway(s) – [RFP 6.2.10]

Although the NENA documents identify scenarios in which the PSAP would use the ESInet to originate SIP calls (e.g., callbacks to original 911 caller) and potentially involve a PSTN Gateway, the PSTN Gateway itself is outside the scope of the NENA i3 model. Further, MIL is requesting several optional call routing features (e.g., see 6.2.14.3) that would require the presence of a PSTN gateway.

Accordingly, BIDDERS are encouraged to provide a PSTN Gateway as a part of their overall solution and a description of its capabilities and/or limitations.

TCS includes PSTN gateways for the purpose of reaching out to non-ESInet entities (e.g., poison control). The gateway is capable of receiving an outbound call and terminating it onto a T1 PRI to route calls from the originating PSAPs out through the ESInet to the PSTN. The PIF function is responsible for this action and is controlled from our [12a] switch acting as the LNG. Therefore, the same highly available architecture we design into the LNG is used for this function.

7.2.11. Statewide GIS Database – [RFP 6.2.11]

At this time there is no statewide 9-1-1 GIS database, accordingly the successful BIDDER shall be responsible for provisioning a GIS database adequate to perform location-based routing to the correct PSAP. Further, while the provision of the Statewide GIS Database is optional, the detailed requirements should be considered “mandatory”,



but no BIDDER will be disqualified for failing to comply with a "mandatory" requirement in this sub section. However, it (non-compliance) may be grounds for rejecting the entire Statewide GIS Database proposal (i.e., this Section) BIDDERS that elect not to include a GIS Database in their proposal must provide a detailed explanation of how a Statewide GIS Database can be introduced into the architecture and impacts to the internal ECRF (and LVF if applicable) GIS database function identified in 6.2.8.6.

[12a]'s solution for a stand-alone GIS function (see response to RFP Section 6.2.8.6) includes development of a statewide GIS database containing the layers listed in Section 6.2.11.4. This solution is easily expandable to include additional layers at a minimum cost.

As described in more detail in Section 6.2.8.6, [12a] will provide ongoing GIS data transformation, aggregation, QA/QC, and reporting which will result in the progressive creation of a single, seamless, statewide GIS dataset. At a high level, these steps will include:

- Each county will submit its GIS data into the SIF via [12a] Server GIS Portal
- Submitted data will be transformed and processed through a series of QA/QC checks
- Any data that does not pass a QA/QC check will be sent back to the county for resolution
- Accepted data will be incorporated into the statewide GIS dataset

This will result in a stand-alone GIS function that can provision to the ECRF/LVF to allow it to route incoming calls to the correct PSAP, as well as provide the framework for developing a single, seamless, statewide GIS dataset with additional layers.

Note: While [12a] will provide regular QA/QC audits, the quality of the GIS data will be the responsibility of county 9-1-1 authorities.

7.2.11.1. GIS Database Availability – [RFP 6.2.11.1]

The GIS database(s) shall be designed and deployed in a manner that affords 5-9's of availability.

We will maintain "five nines" of availability, as the [12a] Server is designed in such a way that no single point of failure will prevent the system from operating.

To further enhance database availability, the dataset is moved to the individual systems running the functional elements of the system. In the unlikely event of a failure, alternative methods of provisioning data [12a] could be used until the system is operational again, while no critical NG9-1-1 functional elements are compromised.

7.2.11.2. ECRF and LVF Access – [RFP 6.2.11.2]

Since the GIS data becomes the key dataset for call routing and location validation, the GIS data must be provisioned and/or made available to the ECRF and LVF (if, and/or when, provided). BIDDERS shall describe all interface, update and support requirements for interfacing a Statewide GIS database to these elements.

The proposal includes contracting with our partner, [12a], to meet the RFP requirements associated with establishing a centralized GIS database.

Each business day, after the GIS data has passed QC, [12a] will upload the file geodatabase that has been [12a] site hosted on the same server as the [12a]. The [12a] GIS technician will notify TCS that the file has been uploaded or that no GIS changes were received.



7.2.11.3. GIS Layers – [RFP 6.2.11.3]

The GIS dataset shall be regularly maintained at the level required to route calls accurately.

While 6.2.11.4 identifies the layers believed to be required in the initial GIS database, the primary GIS layers required for long term routing and validation are:

- Road Centerlines
- PSAP Boundaries
- Site/Structure Addresses (optional)
- State boundaries
- County Boundaries
- Emergency Service Boundaries (EMS, Fire, Law enforcement)
- Municipal Boundaries
- Unincorporated Community Boundaries
- Neighborhood Boundaries (subdivisions, gated communities, etc.)

At a minimum, GIS datasets for ECRF and LVF require PSAP and first responder boundaries, and road centerlines. Road centerlines are required for geocoding civic address locations (i.e., city-style street addresses such as 123 main St.) during 9-1-1 calls. Centerline road names and address range information must be MSAG-valid.

More detailed address information, such as site structure address location, help pinpoint locations and are highly desirable. The ECRF and LVF queries shall be configured to use a hierarchy of data queries based upon the data available for a jurisdiction. Therefore, if the GIS data includes site structure locations, the ECRF and LVF shall query that GIS layer first for a civic address match before querying the road centerline ranges. If there are no site structure points, then the query shall default to geocoding on the road centerline address ranges.

The long-term vision of NG9-1-1 is to provide “sub-parcel polygon features”, which can be divided down to building, floor, seat, etc. BIDDERS should describe if and how their solution would support this fine granularity as data becomes available.

[12a] solution will allow for the inclusion of all the primary GIS layers described above. All layers included in the SIF will use automated schema and geodetic transformation procedures to assimilate the source GIS data layers into a data model that is compliant with NENA’s emerging and evolving NG9-1-1 data standards. As such, subparcel data will be supported as it becomes available from counties, regions, or the state.

7.2.11.4. Minimum Initial Base Data – [RFP 6.2.11.4]

At a minimum the Database shall be initially populated with:

- Street/Road Centerline
- PSAP Boundary
- County Boundary
- Emergency Service Zone (with associated ESN)

TCS is partnering with [12a] whose solution will include these four layers within the statewide GIS dataset. If not available from the state, individual counties, or regional authorities, [12a] can populate the street/road centerline and county boundary layers based upon publicly available sources (such as [12a]). PSAP and ESZ boundaries will be populated based on layers provided by the state, counties, or regional authorities.



7.2.11.5. Hardware and Software – [RFP 6.2.11.5]

BIDDERS shall describe the hardware and software that will be used to provision a GIS database for the entire state.

TCS' partner, [12a], will provide subscription-based access to the following enterprise GIS data management tools, to be hosted in [12a]:

- [12a] GIS Portal for easily transferring GIS data and viewing GIS update status
- [12a] Discrepancy Viewer to efficiently communicate GIS data errors to counties and regional authorities for resolution

7.2.11.6. Database Maintenance – [RFP 6.2.11.6]

The acquiring or creation of base data and then the maintenance of GIS data will be performed by the successful BIDDER. There will be many datasets in Washington at both local and state levels, as well as commercially available data. BIDDERS shall describe how the initial base GIS data will be acquired, validated, synchronized, and updated, and shall describe the experience the BIDDER has in performing these functions.

TCS' partner, [12a], will create an initial statewide GIS dataset for NG9-1-1 by combining GIS data layers from local entities (e.g., counties). [12a] preferred method of local data submission from individual counties or regional authorities is [12a]. Entities unable to upload data via this method will have the option to use [12a] replication to submit data to [12a].

This initial GIS dataset will be statewide, in that it will incorporate existing data throughout the state.

[12a] will implement a QA/QC process that automatically reports GIS errors back to the authoritative source (as described in Section 6.2.12.4) for correction. As counties, regional authorities, and/or the state improve their data based on these error reports, the GIS dataset will become increasingly more complete.

The proposed system accommodates differing data models and geodetic systems from disparate 9-1-1 GIS data sources.

Once received, source GIS data will be run through rigorous QC checks to ensure it meets the state of Washington's NG9-1-1 criteria. Any issues detected will be referred back to source 9-1-1 entities for resolution.

To facilitate the creation of a uniform statewide GIS base map, automated schema and geodetic transformation procedures will be executed to assimilate the source GIS data layers into the authoritative statewide GIS data model. If available, the individual GIS data layers referenced in 6.2.11.3 will then be merged into a statewide dataset.

Once aggregated, the statewide GIS dataset will be loaded into the SIF. As part of this process, [12a] will:

- Create, configure, and load [12a] locators for simple address lookups
- Design [12a] map documents ([12a]) for [12a] (layers, layer order, layer visibility, scale dependent display, symbology, labeling, etc.) based on project stakeholders' preferences



- Develop, configure, test, and publish [12a] Server map services

[12a] has proven experience in developing and implementing multiple statewide and regional datasets in the manner being proposed for the state of Washington, including projects for the states [12a]. The state will be provided with a process and tools to create a dynamic GIS dataset that is continuously improved over time as counties and regions update their data into the system, ensuring that the data to be provisioned to the ECRF is always the most current and accurate data available.

7.2.11.7. Database Maintenance – [RFP 6.2.11.7]

The base GIS data must be maintained on a regular basis, and successful BIDDER must provide a process for updates and corrections to be received, validated, and implemented. These requests for change shall be processed within 24 hours. BIDDERS shall describe the processes and tools used to perform these updates.

TCS is partnering with [12a], whose solution will create an automated process whereby requests for changes submitted with no fatal QC errors will be sent to TCS for processing into the ECRF within [12a]. Requests for change that do contain fatal errors will be evaluated within [12a] and returned to the county for resolution.

To establish this process, [12a] will work with the state and local stakeholders to create a maintenance workflow. Once the initial statewide database has been created, [12a] will provide GIS managed services to ensure the statewide database is continuously updated with improved data submitted by local authorities.

Maintenance Workflow Development

During the same trip as the project initiation meeting, [12a] will host an on-site extract/transform/load (ETL) and GIS data management collaboration meeting, to be held at the same site as the initiation meeting.

[12a] project manager will work with project stakeholders to identify GIS data sources for the system as well as key roles in the GIS data workflow process. In addition, the following will be discussed:

- Existing GIS workflows within the state of Washington
- GIS data quality expectations and data remediation requirements
- Local data source field mapping to statewide accepted data schema
- Developing mechanisms to work toward a true seamless, gapless, statewide dataset through guidelines and standard operating procedures for local jurisdictions maintaining the source GIS data
- Workflows that will allow for changes without fatal QC errors to be consistently processed within [12a]

[12a] will conduct an initial GIS workflow analysis. Local GIS data sources as well as specific roles and responsibilities in the GIS data exchange process will be documented. Existing workflows will be reviewed and modifications will be identified to incorporate the software and services included with the solution.



After the review, [12a] will develop and provide a preliminary copy of the enhanced and new maintenance workflow diagrams. The recommended NG9-1-1 GIS workflows will cover roles, responsibilities, and activities, including:

- Local authoritative GIS data update incorporation, including reviewing, tracking, and management by source 9-1-1 entities
- Review, editing, and management of addressing information from other authoritative sources by source 9-1-1 entities
- Provisioning GIS updates into the regional or statewide GIS dataset
- Workflow for handling QA/QC error reports and subsequent re-provisioning
- Identifying mechanisms for propagating GIS changes to the ECRF/LVF servers

Maintenance Workflow Presentation

After project stakeholders have had time to review the preliminary documentation, the GIS project manager will travel on-site for a one-day working session (extendable to two days if two locations in the state are needed). This will be followed by up to two additional conference calls and/or working web sessions to discuss and adjust the preliminary maintenance workflow diagrams. The final maintenance workflows will be distributed and discussed during an on-site meeting with stakeholders involved in GIS data editing, data management, and submission.

During this same on-site meeting, the GIS project manager also will provide a train-the-trainer training session focusing on how to incorporate [12a]'s GIS data management tools into the new maintenance workflows. Training curriculum includes:

- Core [12a] Server tool functionality
- GIS data request management
- Downloading GIS data from the GIS Portal
- [12a] Discrepancy Viewer functionality
- Accessing QA/QC reports via the GIS Portal or [12a] Discrepancy Viewer
- Managing QA/QC exceptions

Training content and materials will be provided to assist participants to train other system users. Support materials – including agendas, training formats, and scheduling – will be reviewed. Training will occur in conjunction with the workflow presentation.

Note: [12a] understands that all communication needs to be coordinated via the vendor and Washington.

Ongoing NG9-1-1 Managed Services

After the finalization of a GIS maintenance workflow and the aggregation of local data into an initial statewide GIS dataset, [12a] will provide ongoing NG9-1-1 managed services to acquire local GIS data updates, perform GIS data transformation and normalization, execute automated QA/QC, and report GIS discrepancies back to authoritative 9-1-1 agencies for



resolution. The most current data will be available to TCS for provisioning updates into the ECRF. This solution includes:

- Access to [12a] enterprise GIS data management tools
- [12a] Server GIS Portal for transferring GIS data, viewing GIS update status, and downloading QA/QC results
- [12a] Discrepancy Viewer to communicate GIS data errors to source GIS agencies for resolution
- Up to [12a] GIS data normalization, QA/QC, and error reporting

Notes: The [12a] Server GIS Portal will be hosted in a secure data center and provided to project stakeholders as a service.

7.2.11.8. ALI/MSAG Synchronization – [RFP 6.2.11.8]

As legacy PSAPs will still require the capability to query an ALI database, all GIS, MSAG and ALI data shall be synchronized. BIDDERS shall describe how their proposed solution will synchronize GIS data with MSAG/ALI data.

TCS' partner, [12a], will provide the state of Washington and local authorities with quarterly (four times per year) reports comparing each county's GIS data to its MSAG and ALI database. A schedule for quarterly delivery of the current MSAG and ALI database for each entity to [12a] will be discussed as part of the GIS data management collaboration meeting. The MSAG and ALI database must be submitted county-by-county. [12a]

First, [12a] will compare the MSAG and street centerline layer. These procedures will verify that street names are spelled consistently and ESN and community attributes are synchronized.

Second, [12a] will compare house number and street name values in the ALI database against the address point and street centerline layers. Road name inconsistencies, incorrect address ranges, and missing address points or road segments will be identified. This process also will compare ESN and community information to confirm whether ALI database addresses locate within the appropriate boundaries in the GIS map data.

These audits will provide local 9-1-1 authorities with the knowledge needed to synchronize their GIS data to the MSAG and ALI database, as well as a metric for measuring progress toward the needed synchronization level. The quality of the data included in the statewide dataset is ultimately the responsibility of individual counties.

7.2.11.9. GIS Data Ownership – [RFP 6.2.11.9]

All GIS data created or purchased during the contract period will become the property of MIL and the respective County 911 Authority and is not to be disclosed to anyone else.

TCS' partner, [12a] will not retain any rights of ownership, copyrights, or distribution rights for the data created or coalesced for the state of Washington. All data will be for use by the state of Washington at its discretion. In addition, [12a] has an established level of security and follows standard operating procedures that eliminate the possibility of unauthorized access to confidential customer data.



7.2.12. Spatial Information Function (SIF) – [RFP 6.2.12]

As mentioned in the previous section, the State of Washington has not finalized plans on how (and if) a statewide GIS will be implemented, including the policies and procedures for creating updating and otherwise maintaining the data. Accordingly BIDDERS response to the previous section (and this section) may play a major role in determining how GIS will manifest in the new ESInet.

Despite the foregoing, and in view of a single statewide ESInet (and the requirements within this RFP) there will not be multiple SIFs interfacing to the ESInet elements (ECRF and LVF) requiring the GIS data. Rather there will be a single (shared) SIF that ultimately interfaces to, and populates, the ECRF and LVF.

Accordingly, while this section identifies the minimum requirements for a “statewide” SIF, BIDDERS are encouraged to describe all capabilities and features of their SIF solution.

Exhibit 153 includes a high-level description of the products and services [12a] proposes to achieve a single SIF for the state.

Exhibit 153. [12a] Products and Services

Software/Service	Description
[12a]	[12a]
[12a] Discrepancy Viewer	Viewer tool giving local entities using [12a] software a means for interacting with GIS error reports directly inside the GIS. Local 9-1-1 entities not using [12a] or those who do not wish to install [12a] Discrepancy Viewer may still receive GIS error reports.
GIS Data Coalescing Services	After data has been loaded into the system, the GIS data layers will be transformed, aggregated, and coalesced into a seamless, state-level GIS dataset.
GIS Maintenance Workflow Development Services	These services identify new NG9-1-1 GIS data management roles and responsibilities for GIS staff at the local, regional, and state level.
QA/QC Services	A formal QA/QC plan will be developed to document the overall approach to QC, including regular communication of QC results to local GIS entities. Details for specific [12a] control processes also will be developed.
GIS Managed Services	Based on the agreed-upon workflows for system operation and frequency of GIS data updates, ongoing GIS data normalization, QA/QC, and SIF provisioning services.

7.2.12.1. SIF Interfaces – [RFP 6.2.12.1]

The interface for provisioning GIS data from the SIF to ECRF/LVF should comply with the requirements of NENA 08-003. However as the referenced material is not yet stable and issues have been identified, BIDDERS shall identify any assumptions (to deal with some of the ambiguities) that were made in the development of their SIF and any interoperability limitations that may have arisen.

TCS’ partner, [12a] has prototyped a NENA 08-003 v1-compliant special interface (SI) OGC/WFS/ATOM ECRF/LVF provisioning feed mechanism. This NENA-defined interface is based on OGC [12a]. However, because this document is not a standard, the authors of the NENA i3 architecture specification currently believe this document is not definitive enough for vendors to build interoperable implementations of the SI layer replication interface, and that a future OGC specification will describe the protocol definitively. In addition, [12a] has determined that the OGC mechanism described in 08-003 v.1 was not designed specifically for the use case required by ECRF/LVF, [12a]

[12a]



[12a] continues to track NENA i3 SI layer replication interface as a future feature on the [12a] product roadmap, but with no new viable and published standards, [12a] has no committed date for delivery.

While new standards are being developed and evaluated within NENA, [12a] has in the meantime developed a high-performance ECRF/LVF GIS data provisioning, update, and replication system built on existing, widely adopted, robust technologies of [12a] Server geodatabase replication and [12a] replication for [12a]

7.2.12.2. 24x7x365 Availability – [RFP 6.2.12.2]

The SIF shall be available on a 24x7x365 basis. While the State is not requiring “5-9’s” as an Availability Factor, BIDDERS shall describe the mechanisms (e.g., redundancy, Off-site data backups/restorals, etc.) employed to insure that this element remains in the realm of “high” Availability.

As well, BIDDERS shall identify the SLA(s) associated with guaranteeing availability and system performance and (proposed) remedial credits as applicable to the solution.

We design our production systems for high availability. The SIF will be similarly maintained using geodatabase replication to diverse sites. The proposed SLAs and credits are outlined below.

SIF SLAs

- **Grace period:** There is a grace period immediately following system provisioning:
 - Remedies for SLA failures are not available for the first [1] days of support while all parties, including those outside [12a]’s control, work out and fix any workflow and/or interface- and interoperability-related issues. (SLAs are post-acceptance remedies.)
 - Service level commitments will be tracked and reported monthly beginning on the first day of the month following customer’s acceptance of the product. (SLAs are post-acceptance remedies.)
- Remedies will not be paid for the first service level violation in a year. For example, if a failure does not occur for six months, the next failure will not be subject to remedies. This rewards [12a] for perfect 100 percent uptime.
- **Reporting:** All [12a] SLAs will be measured and monitored by [12a]. By the 5th of each month a monthly report will be provided for downloading stating if SLAs have been met for the prior month. This report would also include any violations and resulting remedies for the previous month. Any remedies that are owed will appear as a credit on the next scheduled invoice to customer.
- **Limitations:** Limits to remedies paid by [12a] are as follows:
 - Remedies are only available if the customer meets [12a] published minimum hardware, software, and network requirements for SIF componentry and service.
 - Remedies are only available if the customer provides [12a] with all necessary information and [12a] can verify the failure.



- Maximum cap on all remedies, including cumulatively for multiple failures, is a service credit in the amount of 5 percent of the total monthly service fee for SIF.

[12a] will perform as Tier 3 Support where emergency calls are addressed 24 hours a day, 7 days a week via a toll-free number/pager system based on mission critical nature of the [12a] solutions implemented as defined in a separately determined escalation plan between [12a] and TCS regarding performance response times.

[12a] defines emergency calls as one or both of the following:

- System alarms where software does not process calls
- System locks up repeatedly without ability to recover

Our response to customer issues is fast because [12a] develops all proposed software components, trains its technicians on advanced troubleshooting methods, can remotely connect to your system, and are able to interact with your software via the web. This results in quicker diagnosis and call closure. Ultimately, this means less downtime and maximum software functionality benefits.

[12a] describes SLAs, metrics, and limitations in Exhibit 154.

Exhibit 154. SLAs, Metrics, and Limitations

SLA	Description	Measurement	Exclusions	Remedy
Availability	SIF is online and users can log into the UI and interact with the system, upload/download GIS data and reports. [12a] guarantees 99% uptime.	More than 1% of unplanned downtime per month.	Approved scheduled maintenance for repair and upgrade, internet outage, and/or customer local environmental issue beyond [12a]'s control.	A service credit in the amount of 5 percent of the total monthly fee for SIF service.
Maintenance Notification (Related to [12a] Products and Services)	Notification of scheduled maintenance event shall be provided at least 10 business days prior to the event.	Number of business days (Monday-Friday, 8 a.m. to 5 p.m. U.S. Central, when [12a] is open for business) in advance of downtime-causing maintenance event that notification is sent to customer.	Maintenance events with less than 10 business days' notification but that are approved by customer in order to expedite maintenance.	A service credit in the amount of 5 percent of the total monthly fee for SIF service.



SLA	Description	Measurement	Exclusions	Remedy
Maintenance Event Duration	Scheduled maintenance events for the SIF shall not [12a]	Duration of downtime-causing maintenance 2 greater [12a]	Availability service level failures triggering Remedy, maintenance events involving non-[12a] software and system hardware such as [12a] operating systems, [12a] for Server.	A service credit in the amount of 5 percent of the total monthly fee for SIF service.

7.2.12.3. Processing Time – [RFP 6.2.12.3]

All (data) inputs must be processed and uploaded to the ECRF/LVF within 24 hours of receipt.

[12a]'s solution will create an automated process whereby GIS data inputs with no fatal QC errors will be processed and sent to TCS for uploading to the ECRF and LVF within [12a]. Requests for change that contain fatal errors will be evaluated within [12a] and returned to the county for resolution. GIS processing and timelines (for example, submission deadlines) will be finalized with the Agency as part of the project implementation.

[12a] will work with the State to establish a daily schedule for updates with a deadline for counties to submit up to daily GIS changes for processing. Data submitted by this daily deadline (our current projects have evening deadlines) would undergo quality control checks and either be provisioned to the ECRF within [12a], submissions that meet the daily timeline will be provisioned in the system by the end of the [12a], or returned to the county for resolution. [12a]

7.2.12.4. Quality Assurance/Quality Control (QA/QC) – [RFP 6.2.12.4]

The proposed solution shall include QA/QC functionality. BIDDERS shall describe the solutions capabilities including any level of automation and closed loop error reporting/feedback mechanisms.

Before GIS data can be used for routing 9-1-1 calls and validating civic locations in an NG9-1-1 system, the data's accuracy and integrity must be validated through a series of data-specific, thorough QA/QC procedures. Without proper QA/QC, GIS data issues could interfere with NG9-1-1 emergency response operations. The QA/QC plan will be discussed during project initiation and GIS data management collaboration meetings.

As part of the GIS maintenance workflow development process, a [12a] GIS project manager will collaborate with project stakeholders to develop a formal QA/QC plan. The QC approach, including regular communication of QA/QC results to local GIS entities, will be documented. The plan also will detail initial ongoing QC processes to be performed on local GIS data submitted to [12a] and into the SIF.

The final QA/QC plan will be submitted to project stakeholders for review and approval prior to initiating any managed GIS services.



When updates are submitted by individual counties, multiple automated and manual QC processes are performed prior to coalescing the updates into the statewide GIS dataset to ensure proper topology and data integrity. These processes may include those shown in Exhibit 155.

Exhibit 155. Manual Quality Control Processes

GIS Data Layer	Associated GIS Quality Control Processes
Road Centerlines	Address Range Audit – to identify overlapping address ranges that could cause addresses to geocode in the wrong location
	Topology Audit – to locate unbroken/unsnapped intersections that could cause routing issues
	Missing Attribute Audit – to identify missing or invalid values in pertinent attribute fields
	Road Name Audit – to ensure proper road name standardization
	Length Audit – to identify road segments which could cause addresses to geocode in the wrong location
Address Points	Address Spacing Audit – to identify duplicate addresses
	Address Missing Attribute Audit – to identify missing or invalid values in pertinent attribute fields
	Address Sanity Audit – to ensure logical assignment of house numbers with respect to centerline
Boundary Layers	Topology Audit – to locate gaps and overlaps in polygon coverage
	Missing Attribute Audit – to identify missing or invalid values in pertinent attribute fields
	Duplicate Audit – to check for duplicate attributes that could interfere with address location
Multi-Layer Topology	Verifies road centerline segments are broken where they cross any ESN, community, or PSAP boundaries, ensuring that addresses (based on address ranges) are properly located within the correct community and ESN on the map. Boundaries that run parallel to road segments should be snapped to those road segments at each vertex.

GIS error reports will be generated for updates that do not pass QC. These reports will be transmitted to the sending agency and, optionally, to stakeholders at the state level for performance monitoring.

7.2.12.5. Data Conversion/Normalization – [RFP 6.2.12.5]

Again, as the State/Counties have yet to establish the policies/procedures, and even the data format(s) that will be used for NG9-1-1 GIS, BIDDERS shall describe the solutions capabilities and limitations (if any) in converting/normalizing received data. Alternatively, BIDDERS could describe the formats and mechanisms that the solutions is already capable of accommodating.

The proposed system accommodates differing data models and geodetic systems from disparate 9-1-1 GIS data sources in any [12a] will draw on experience in past statewide projects to assist the state and the local stakeholders with the development of the statewide NG9-1-1 data schema if this has not yet been finalized. The data schema will need to be



finalized during the ETL and GIS data management collaboration meeting, as it will provide the base for the ETL processes to be developed by [12a]

After the initial data load, [12a] method for submitting GIS data updates into the system is through the [12a]. Entities unable to upload data to the [12a].

When a county submits a GIS update to [12a] automatic validation checks are performed to ensure the dataset meets the minimum requirements for further processing.

7.2.12.6. Performance Measurements – [RFP 6.2.12.6]

BIDDERS shall identify what performance measurements are associated with their solution. Performance measurements being defined as those metrics necessary to ensure all components of the SIF are operating as required for NG9-1-1, including human workflows and processes.

TCS’ partner, [12a], will provide quarterly reports to the state of Washington, in PDF format, transmitted via email. The reports will summarize key system metrics and will contain, [12a], the data points shown in Exhibit 156.

Exhibit 156. Data Points Contained in [12a] Quarterly Reports

Performance Report Element Type	Description	Metrics
GIS Data Performance	[12a]	
GIS Data Performance		
GIS Data Performance		
GIS Data Performance		
Service Level		
Service Level		
Service Level		
Service Level		
Service Level		
Service Level		

At the beginning of the project, TCS and [12a] will work with the state to identify any additional items that can be prepared in the ordinary course of business and should be included in the quarterly report. We will include third-party computed availability statistics with the availability SLA report as appropriate.



7.2.13. Security [RFP 6.2.13]

In addition to any specific security measures identified elsewhere within this RFP, and the following, BIDDERS are encouraged to provide additional information on any additional security measures taken to insure the safe and secure operation of the ESInet.

7.2.13.1. NENA NG-SEC 75-001 – [RFP 6.2.13.1]

BIDDERS shall provide a compliance matrix, by Section/Sub-Section, that identifies whether their proposed solution, Complies (C), or Complies with Exceptions (CE), Non-Compliant (NC) or is Not Applicable (NA) to the identified requirement(s). Not Applicable shall be used when the BIDDERS proposal does not contain the functionality contained therein (for example, if the Proposed Solution does not support “Wireless Access” (Section 6.4.6 of 75-001), then the section is “Not Applicable”).

We have provided a compliance matrix, by section and subsection, as required. [12a]

[Redacted]

[Redacted] In addition to compliance to NG-SEC, we also are ISO 27001 (Information Security Management) certified.

The matrix provided by TCS in this section includes information about the TCS solution’s compliance with NENA NG-SEC 75-001. [12a]

[Redacted]

Exhibit 157 below shows how TCS complies with NENA NG-SEC 75-001 as revised for the 5/4/2016 meeting with MIL.

Exhibit 157. NENA NG-SEC 75-001 Compliance

Section/Subsection (NENA NG-SEC 75-001)	Compliance	Comments
4 Security Policies	[12a]	
4.1 Senior Management Statement of Policy		
4.2 Functional Policies		
4.3 Procedures		
5 Information Classification and Protection		
5.1 Overview		



Section/Subsection (NENA NG-SEC 75-001)	Compliance	Comments
5.2 Roles and Responsibilities In Information Classification and Protection	[12a]	
5.3 Information Classification Guidelines		
5.4 Protective Sensitive Information		
5.5 Default Classification		
5.6 Authorizing Access to Information		
5.7 Safeguarding Electronic Information		[12a] [REDACTED]
5.8 Transport and Shipping of Electronic Media and Devices		
5.9 Safeguarding Printed Information/Material		
5.10 Sensitive Information Destruction & Sanitization		
6 General Security		
6.1 General Responsibilities		
6.2 Application, System and Network Administrator Responsibilities		
6.3 Ensuring Compliance for Recurring Security Requirements		
6.4 Network Connectivity Requirements		
6.5 Security Training		
6.6 Suspicious Activity		
6.7 General Guidelines		
7 Safeguarding Information Assets		
7.1 Identification and Authentication		
7.2 Access Control		
7.3 Confidentiality		
7.4 Integrity		
7.5 Availability		[12a] [REDACTED]
7.6 Audit and Accountability		
8 Physical Security Guidelines		



Section/Subsection (NENA NG-SEC 75-001)	Compliance	Comments
8.1 Building and Physical Access Control	[12a]	
8.2 Authorized Physical Entry		[12a] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
8.3 Storage Media and Output		
8.4 Mobile Devices		
8.5 Environmental Controls		
8.6 Server Room		
8.7 Data Communications Networks		
9 Network and Remote Access Security Guidelines		
9.1 Firewalls/Security Gateways		
9.2 Remote Access		
9.3 Extranet and External WAN Connectivity		
9.4 Intrusion Detection/Prevention		
9.5 Layer 2 Security and Separation		
9.6 Network Redundancy and Diversity		
10 Change Control and Documentation		
11 Compliance Audits and Reviews		
12 Exception Approval and Risk Acceptance Process		
12.1 Exception Approval and Risk Acceptance Process Scope		
12.2 Roles and Responsibilities in the Exception Approval and Risk Acceptance Process		
12.3 Process		
12.4 Review Period		
12.5 Change of Circumstance		

7.2.13.2. OCIO Policy 141.10 – [RFP 6.2.13.2]

BIDDERS shall provide a compliance matrix, by Section/Sub-Section, that identifies whether their proposed solution, Complies (C), or Complies with Exceptions (CE), Non-Compliant (NC) or is Not Applicable (NA) to the identified requirement(s). Not Applicable shall be used when the BIDDERS proposal does not contain the functionality contained therein (for example, if the Proposed Solution does not support “Wireless Access” (Section 6.4.6 of 75-001), then the section is “Not Applicable”).

- Non-Compliant
 Compliant with Exceptions
 Compliant



Below is TCS' compliance table for the Washington Office of the Chief Information Officer (OCIO) 141.10.

Exhibit 158 below shows how TCS complies with the Washington OCIO policy as revised for the 5/4/2016 meeting with MIL.

Exhibit 158. Washington OCIO Policy Compliance

Section/Subsection (OCIO 141.10)	Compliance	Comments
1 IT Security Program	[12a]	[12a]
1.1 Documentation		
1.2 IT Risk Assessment		
1.3 Security Assessment		
1.4 Education and Awareness		
1.5 Compliance		
1.5 Maintenance		
1.6 Audit		
2 Personnel Security		
3 Physical and Environmental Protection		
3.1 Facilities		[12a]
4 Data Security		
4.1 Data Classification		
4.2 Data Sharing		
4.3 Secure Data Transfer		
5 Network Security		
5.1 Secure Segmentation		
5.2 Restricted Services		
5.3 External Connections		
5.4 Wireless Connections		
5.5 Security Patch Management		
5.6 System Vulnerabilities		
5.7 Protection from Malicious Software		



Section/Subsection (OCIO 141.10)	Compliance	Comments
5.8 Mobile Computing	[12a]]	[12a] [Redacted]
6 Access Security		
6.1 Access Management		
6.2 Password Requirements		
6.3 Authentication		
6.4 Remote Access		
7 Application Security		
7.1 Planning and Analysis		
7.2 Application Development		
7.3 Application Maintenance		
7.4 Vulnerability Prevention		
7.5 Application Service Providers		
8 Operations Management		
8.1 Change Management		
8.2 Asset Management		
8.3 Media Handling and Disposal		
8.4 Data and Program Backup		
9 Electronic Commerce		
10 Security Monitoring and Logging		
10.1 Logging Policies		
10.2 Logging Systems		
10.3 Intrusion Detection and Prevention		
11 Incident Response		[12a] [Redacted]



7.2.13.3. Independent Third-Party Security, Availability, and Confidentiality Audits – [RFP 6.2.13.3]

MIL requires that all BIDDERS acknowledge that agreement to conduct and facilitate independent third-party security, availability & confidentiality audits will be a condition of contract award. MIL expects that the initial audit will be a part of the Acceptance Test Plan (ATP) and then optionally conducted on a 3-5 year cycle.

7.2.13.3.1. A mutually agreed upon third-party auditor will perform audits on a three-year cycle but understands MIL may incorporate additional mutually agreed to metrics to the audit checklist. Third-Party Security Audit(s) Basis – [RFP 6.2.13.3.1]

NENA "Next Generation 9-1-1 Security (NG-SEC) Audit Checklist (NENA 75-502) shall form the basis for the security audits identified in 6.2.11.2. MIL reserves the right to incorporate any additional metrics identified by the 3rd Party auditor.

TCS complies with the requirement for security to be evaluated using the NG-SEC audit checklist, and understands Washington may incorporate additional metrics to the audit checklist.



7.2.14. Basic Call Processing – [RFP 6.2.14]

Basic Call Processing shall be in accordance with the Functional Requirements identified within Section 4 of 08-751 “NENA i3 Technical Requirements Document”.

BIDDERS shall provide a compliance matrix, by Section/Sub-Section/Requirement, that identifies whether their proposed solution, Complies (C), or Complies with Exceptions (CE), Non-Compliant (NC) or is Not Applicable (NA) to the identified requirement(s). Instances of CE and NA shall respectively identify the exception(s) and reason(s) the requirement is NA. Non-compliance with requirements not applicable (for example, Signaling 1100-0100 – there are no Selective Routers remaining in Washington state) to the BIDDERS proposal will not automatically result in BIDDER disqualification.

The [12a] solution complies as follows with NENA 08-751 Section 4, as detailed line-by-line in the compliance matrix shown in Exhibit 159 below.

The 08-751 document is adhered to in all major aspects, with any deviations noted in our response. Our overall compliance to the requirements is very high, and any exceptions are either by design to fulfill needs unaddressed in the document, equivalent designs, or items that are not applicable.

The matrix provided by TCS in this section includes information about the TCS solution’s compliance with NENA 08-751. This level of detail on compliance of TCS’ technology is not necessarily known to TCS’ business competitors and could be used by business competitors to the competitive disadvantage of TCS. Accordingly, TCS believes that such information should be protected as financial, commercial, and/or proprietary information belonging to TCS exempt from public disclosure pursuant to the provisions of RCW 42.56.270, and should be redacted from any public records disclosure of the TCS proposal this SOW or Contract. In addition to and notwithstanding the status of such information as financial, commercial, and/or proprietary information belonging to TCS as described above, TCS also notes that the Agency may wish to consider limiting public disclosure of such portions of TCS’ response based on general concerns for public security and safety and pursuant to the exemption of specialized details of security arrangements from public disclosure permitted pursuant to the provisions of RCW 42.56.420(4). Notwithstanding anything to the contrary, the terms of this SOW and this Section are remain subject to Sections 8.2 and 8.5 of the Contract.

Exhibit 159. Basic Call Processing Compliance Matrix

NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
4.1 Calls Directed to a PSAP	[12a]	
4.1.1 Signaling		
Signaling 0100-0100 Session initiation (call) signaling for IP connected callers shall initially be SIP based. Other protocols are permitted if they are interworked to SIP for presenting to the PSAP. PSAPs shall not be required to accept IP calls using any protocol other than SIP. The architecture shall permit evolution to future protocols.		



Washington State Military Department
 Next Generation 9-1-1 Emergency Services Internet Protocol Network
 Statement of Work | June 24, 2016

NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Signaling 0200-0100 Signaling shall be supportable over UDP and TCP with or without TLS security. PSAP policy shall govern which of these transport mechanisms are acceptable.	[12a]	
Signaling 0300-0100 Abandoned calls shall be captured, with location (if available) and call back information (address or TN as applicable) for presentation to the call taker.		
Signaling 0400-0100 Tracking and Tracing Facilities for all calls must be provided. These include all routing entities as well as all signaling entities.		
Signaling 0500-0100 Each element in conforming i3 implementations shall maintain call detail records that can be accessed by management systems to develop call statistics in real time.		
Signaling 0600-0100 The PSAP shall be able to optionally control disconnect.		
Signaling 0700-0100 Conforming i3 implementations must harmonize with international specifications to permit local determination of emergency call number (i.e. 9-1-1, 1-1-2)		[12a]
Signaling 0800-0100 Mechanisms must be provided to route calls to areas not served by E9-1-1 to an appropriate PSTN telephone number		
Signaling 0900-0100 Each element of conforming i3 implementations shall provide congestion controls		
Signaling 1000-0100 It shall be possible to determine the complete call chain of a call, including the identity of each signaling element in the path, and the reason it received the call, e.g. alternate routed. (This is an existing SIP mechanism, Call History).		[12a]
Signaling 1100-0100 The Emergency Services IP Network or the PSAP must accept calls from selective routers, including CAMA-like and ISDN interfaces		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Signaling 1200-0100 POTS users must be capable of placing emergency calls through gateways to IP based systems.	[12a]	
Signaling 1300-0100 Support must be provided to accept calls from end offices and MSCs where selective routers are no longer provided [12a]		
Signaling 1400-0100 Call setup time (dialing of last digit to ring at the PSAP), under expected peak load shall be less than 2 seconds. If CAMA-like signaling is in the path, then an additional 7 seconds is permitted.		
Signaling 1500-0100 Voice Activity Detection1 shall be disabled for emergency calls.		
4.1.2 Media		
Media 0100-0100 PSAPs shall accept voice, video and text media streams on RTP transport		[12a]
Media 0200-0100 The Emergency Services IP Network or the PSAP must support existing TTY devices,		
Media 0300-0100 PSAPs shall have facilities to detect and react to silent calls		[12a]
Media 0400-0100 It shall be possible for PSAPs to supply ringback media to callers		[12a]
Media 0500-0100 It shall be possible for PSAPs to accept additional media (e.g. images) from callers without tearing down the call.		[12a]
Media 0600-0100 A minimal (e.g. DiffServe) QoS mechanism shall be specified for use for media presented to or originated from the PSAP.		
Media 0700-0100 i3 elements which originate media shall have media loopback mechanisms.		
4.1.3 Location		
Location 0100-0100 Calls using VoIP or subsequent methods are expected to supply location with the call.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Location 0200-0100 PSAPS shall accept location as civic and/or geo specified	[1 2a]	
Location 0300-0100 The format for location shall be PIDF-LO		
Location 0400-0100 All representations of location shall include the capability to carry altitude and/or floor designation. This requirement does not imply altitude and/or floor designation is always used or supplied		
Location 0500-0100 Altitude and/or floor designation shall be provided if available.		
Location 0600-0100 The minimum required coordinate basis is WGS-84 or better		
Location 0700-0100 The solution shall specify when multiple locations are permitted, what the interpretation of multiple locations shall be, and what the functional elements must do with the locations.		[12a]
Location 0800-0100 No assumption shall be made that the entity presenting the call to the PSAP has any knowledge of, or control over the provider of location. The location provider may be independent of all other service providers handling the call.		
Location 0900-0100 The location source shall be identified and should be Authenticated.		
Location 1000-0100 Systems which deploy external LISs that use keys shall provide intermediaries to query the LIS and supply the PSAP with location. The PSAP is not expected to query a LIS with a key in order to determine location.		
Location 1100-0100 PSAPs shall have the ability to requery for a location update.		
Location 1200-0100 PSAPs shall have the ability to subscribe to an automatic location update event for a particular call		[12a]
Location 1400-0100 PSAPs shall be able to make use of fallback location information when measurement based location determination mechanisms fail. Examples include tower/Access Point location, last known fix, etc.		[12a]



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Location 1500-0100 PSAPs must be made aware when fall back location information was used to route a call or when it is presented to the call taker as location data.	[12a]	[REDACTED] [12a] [REDACTED] [REDACTED]
4.1.4 Call Back Address		
CallBack 0100-0100 Calls to 9-1-1 shall supply a call back address (URI, which includes the possibility of an E.164 TN expressed as a tel URI) with the call		[REDACTED] [12a] [REDACTED] [REDACTED]
CallBack 0200-0100 Calls must provide both a permanent address that reaches the caller and, if different, a temporary address to immediately reconnect to the caller if the call is dropped		[REDACTED] [12a] [REDACTED] [REDACTED]
Note: The PSAP may not receive a conventional telephone number. In the case of a VoIP caller, the URI may not have a telephone number. This has implications on how and to what extent backwards compatibility can be provided.		
4.1.5 Additional Information		
In addition to information sent with the call, additional information may be available that is retrieved from internal or external databases using information included with the call as a key. NENA's Future Path Plan (FPP) provides a useful classification of data that may be used to classify such data. It proposes three categories:		
<ul style="list-style-type: none"> • Tier 1 (Essential) 		
<ul style="list-style-type: none"> • Tier 2 (Supportive) 		
<ul style="list-style-type: none"> • Tier 3 (Supplemental) 		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
<p>Tier 1 information is defined as “data that supports call delivery and adequate response capability.” Examples include callback number and caller location. Tier 2 information is defined as information beyond essential data that may support call handling and the dispatch of a call. An example of this type of data may be vehicle information such as “vehicle rolled.” Tier 3 information may supplement the call handling and dispatch, but is not necessary to complete the handling of the situation. An example may be personal medical information. Generally, we expect Tier 1 data, or a reference to it, to be delivered with the call, and Tier2/Tier 3 data be available within the Emergency Services IP Network, or elsewhere, to be subscribed to or queried by the PSAP when needed. Such additional (Tier 2 & 3) data may also be made available to the PSAP proactively by other entities via the ESInet, meaning that the PSAP may not need to ask for it, although they would always have the ability to disregard or refuse to receive it.</p>	<p>[12a]</p>	
<p>AddInfo 0100-0100 Additional information may be available to the call taker based on the location of the caller, see section 4.2.1</p>		<p>[12a]</p>
<p>AddInfo 0200-0100 Additional information may be available to the call taker based on the owner of the structure, see section 4.2.1</p>		<p>[12a]</p>
<p>AddInfo 0300-0100 Additional information may be available to the call taker based on the tenant of the structure, see section 4.2.1</p>		<p>[12a]</p>
<p>AddInfo 0400-0100 Where a vehicle is involved, additional information may be available, see section 4.2.1</p>		<p>[12a]</p>
<p>AddInfo 0500-0100 Additional information may be available based on the Address of Record (AoR) of the caller. In this context, AoR equates to the caller</p>		<p>[12a]</p>
<p>AddInfo 0600-0100 Consideration should be given to permitting callers to have domain independent mechanisms to supply information or the scene of the incident about themselves</p>		<p>[12a]</p>
<p>4.1.6 Calls placed by a third party</p>		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
<p>Calls may be originated by an entity, typically a call center on behalf of a caller. Examples include telematics, central alarm monitoring, text or video relay, and satellite systems. 3rd party call origination requires that the call be routed based on the location of the caller, and not the location of the 3rd party. Not all callers, or all 3rd parties may be VoIP capable, and some calling mechanisms (such as some Telematics systems) do not have the capability for direct call back. Thus the originator may not be able to support all of the capabilities described here.</p>	[12a]	
<p>3rdParty 0100-0100 3rd party originated calls shall be fully supported in conforming i3 implementations</p>		
<p>3rdParty 0200-0100 PSAPs should receive an indication with the call that it is a 3rd party call</p>		[12a]
<p>3rdParty 0300-0100 PSAPs should receive the identities of all other parties in the call. This may need to be specific to an operator in a 3rd party call center.</p>		[12a]
<p>3rdParty 0400-0100 The call should include callback information for both the caller and the 3rd party such that the PSAP can recreate the call if it is dropped.</p>		[12a]
<p>3rdParty 0500-0100 The 3rd party shall be able to provide supplemental information, either with the call directly, or a reference to it.</p>		[12a]
<p>3rdParty 0600-0100 Location of the caller may come from access network of the caller or from the 3rd party</p>		
<p>3rdParty 0700-0100 3rd parties may need authorization through an administrative process before they can place 9-1-1 calls</p>		
<p>4.1.7 Validation of Civic Location</p>		
<p>Validation 0100-0100 It must be possible to determine, BEFORE an emergency call is placed, if a civic address is valid.</p>		[12a]
<p>Validation 0200-0100 A "9-1-1 Valid Address Database", which contains all valid street addresses within a defined area, should be used as the basis to determine validity of a civic address</p>		
<p>Validation 0300-0100 A 9-1-1 valid address is defined as an address with a subset of the fields in the NENA XML address format, which when looked up in the 9-1-1 Address Validation database, yields exactly one record. This requirement does not preclude the validation mechanism from returning multiple 9-1-1 valid locations.</p>		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Validation 0400-0100 If it is determined that an address is invalid; an error diagnosis should be supplied to the querier if appropriate, as well as a contact URI for resolving errors in the database.	[12a]	
Validation 0500-0100 Methods must be provided to revalidate locations to accommodate changes to the 9-1-1 valid address data.		
Validation 0600-0100 The 9-1-1 Valid Address Database defined area boundaries may have the same characteristics as Routing 0800-0100, Routing 0900-0100 and Routing 1000-0100 below.		
Validation 0700-0100 Validation information must be secured against unauthorized modification. 9-1-1 Authority3 (or perhaps a higher level civic authority such as a county, state/province or national body) must be the only entities permitted to make changes to the database.		
Validation 0800-0100 The fields in the 9-1-1 Valid Address Database must be used as they are defined in the relevant NENA Standard, including use of the Street suffix, pre and post directionals, etc. Only USPS abbreviations will be permitted in suffixes. No abbreviations are permitted in street names or community names. All fields must be populated as appropriate, including the postal community name, county name, and zip code.		
Validation 0900-0100 PSAPs must have access to the actual (MSAG) community name		
Validation 1000-0100 i3 must define a process to evolve from the current MSAG to the 9-1-1 Address Validation database		
Validation 1100-0100 A postal address may be a 9-1-1 valid address if, as stated in Validation 0800-0100, a query to the 9-1-1 Address Validation Database with the postal address yields exactly one record. This requirement does not preclude the validation mechanism from returning multiple 9-1-1 valid locations.		
Validation 1200-0100 A current MSAG address may be a 9-1-1 valid address if the fields are fully populated as described in Validation 0800-0100 (with respect to, for example, mandatory use of street suffix and pre/post directionals, only standard USPS abbreviations permitted, etc.)		
Validation 1300-0100 The PSAP must have access to all of contents of the 9-1-1 address validation database.		
4.1.8 Routing of Calls		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Routing 0100-0100 Calls must be routed to the correct PSAP based on the location of the caller known at the time of the call and the declared service boundary of the PSAP	[12 a]	
Routing 0200-0100 Routing must be possible on either civic or geo		
Routing 0300-0100 It must be possible to route a call from either a civic or a geo without requiring conversion. This requirement does not prohibit an implementation from converting and using the resulting conversion for routing. However, see Req 0600-0100		
Routing 0400-0100 It must be possible for a designated 9-1-1 authority to approve of a geocoding database used to convert civic to geo as part of determining how to route calls to it. Mechanisms must be provided for a PSAP to test, and certify a geocoding database as suitable for routing calls to it. The PSAP may choose to NOT avail itself of such a mechanism.		
Routing 0500-0100 It must be possible for the designated 9-1-1 authority to supply, maintain, or approve of databases used for civic routing including geocode data if civic routing is achieved by geocoding a civic address. Mechanisms must be provided for a PSAP to test and certify a civic routing database as suitable for routing calls to it.		
Routing 0600-0100 There must be a database (K6) interface defined so that the PSAP itself (or a contractor it nominates on its behalf) may provide geocode and reverse geocode data (off line, not in real time). This implies definition of a standard interchange format for geocode data, and protocols to access it.		
Routing 0700-0100 There must be a mechanism to declare PSAP serving boundaries (in civic and geo formats) for routing purposes (e.g. to the administrative interface of the call routing mechanism).		
Routing 0800-0100 Boundaries for civic routing must be specific to a street address range, a side of a street (even/odd street addresses), a building within a "campus", or any of the location fields available.		
Routing 0900-0100 It must be possible to use various components of the location object for determination of routing. Some areas may only require routing to a country level, others to a state/province, others to a county, and so on. No assumption should be made on the granularity of routing boundaries.		
Routing 1000-0100 Boundary mechanisms for geo routing must be able to be specific to a political boundary, a natural physical boundary (such as a river), or the boundaries listed in Req 0900-0100 above		



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

NENA 08-751 Section 4 Functional Requirement	Compliance	Comments	
Routing 1100-0100 Routing databases using 9-1-1 Valid Addresses or lat/lon/altitude as keys must be available to all entities needing to route 9-1-1 calls	[12a]		
Routing 1200-0100 Carriers, enterprises and other entities that route emergency calls must be able to route calls to the appropriate Emergency Services Network based on available location information. There must be no restrictions on call originators.			
Routing 1300-0100 It must be possible for any given 9-1-1 Authority to decide where its calls should be routed, and make changes to its routing policy dynamically.			
Routing 1400-0100 It shall be possible for higher level civic authorities such as a county or state/province to be able to make common routing decisions for all PSAPs within their jurisdiction. For example, a state may wish to have all emergency calls placed within that state directed to a specific URI. This does NOT imply a single answering point; further routing may occur beyond the common URI.			
Routing 1400-200 It shall be possible that certain routing information only be accessible by authorized entities			
Routing 1500-0100 It shall be possible to change routing may change on short notice due to local conditions, traffic, failures, schedule, etc.			
Routing 1600-0100 This requirement has been deleted			[12a]
Routing 1700-0100 Routing information must be secured against unauthorized modification. PSAPs (or perhaps a higher level civic authority such as a county, state/province or national body) must be the only entities who can authorize a change to routing information			
Routing 1800-0100 It must be possible to supply contingency routing information, for example, an alternate URI or an E.164 to be used when normal routing fails.			
Routing 1900-0100 Multiple types of failures may have different contingency routes			
Routing 2000-0100 It must be possible to provide more than one contingency route for the same type of failure			
Routing 2100-0100 A procedure must be specified to handle "default route" capability when no location is available or the location information is corrupted			



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Routing 2200-0100 Location available at the time the call is routed may not be accurate. Updates to location may result in a different route and the system must accommodate this. If the call has not been answered before the update is available, the system may reroute the call automatically. After the call is answered, the PSAP may request the call be rerouted as part of a transfer operation.	[12a]	[12a] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted]
Routing 2300-0100 This requirement has been deleted		[12a]
Routing 2400-0100 Access Infrastructure providers must provide a location object that is as accurate as possible when location measurement or lookup mechanisms fail.		[12a]
Routing 2500-0100 Entities routing emergency calls shall retain information used to choose a route for subsequent error resolution		
Routing 2600-0100 It should be possible to have updates of location (which may occur when measuring devices provider early, but imprecise "first fix" location) change routing of calls. See Routing 2200-0100.		
Routing 2700-0100 There shall be mechanisms to route calls to one or more alternate PSAPs when a PSAP receives a very large number of calls (which is an instance of alternate-routing)		
Routing 2800-0100 Alternate-routing shall be able to be initiated by an authority designated by the PSAP		
Routing 2900-0100 There shall be mechanisms to allow PSAPs to accept or refuse such alternate-routed calls. No calls shall be alternate routed to another PSAP where the destination PSAP does not accept such routing		[12a] [Redacted] [Redacted]
Routing 3000-0100 Prior arrangements for alternate-routing calls shall be possible, but provisions must be made for dynamically changing such arrangements		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Routing 3100-0100 Alternate-routed calls shall be capable of being bridged back to the original destination PSAP if appropriate	[12a]	
Routing 3200-0100 Alternate-routed calls shall be recognizable as alternate-routed before they are answered at a PSAP		
Routing 3300-0100 Alternate-routing mechanisms should be designed to function well in disaster situations where loss of connectivity will be common		
Routing 3400-0100 There shall be mechanisms to carry the reason for alternate routing (differentiating for example on incoming call queue busy from failure of an element) and make different routing decisions based on the reason.	[12a]	<p>[12a]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Routing 3500-0100 PSAPs shall be able to specify treatment of its calls in all abnormal situations, where treatment includes return of busy indication, answering at an alternate PSAP, connection to an Interactive Voice Response Unit, etc.		
Routing 3600-0100 PSAPs shall be able to accept non-emergency calls placed to, for example 3-1-1		
4.1.9 Connections to the Emergency Services IP Network		
Connections 0100-0100 If there is network connectivity between the emergency caller and a PSAP, and routing information is available, the call should go through, even if other parts of the network are not reachable.		
Connections 0200-0100 PSAPs shall have functions to determine the status of the Emergency Services IP Network		
Connections 0300-0100 It must be possible to connect directly, via IP, to the Emergency Services IP Network, or indirectly via the Internet		
4.1.10 Support of existing wireline and wireless callers		
Existing 0100-0100 Backwards compatibility of existing wireline and wireless callers must be implemented		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Existing 0200-0100 Support mechanisms for backwards compatibility may evolve, but at all times it must be possible to accommodate existing originating offices and mobile switching centers without requiring changes to such switches.	[12a]	
4.2 Databases and Services available to the PSAP to handle Calls		
i3 includes interfaces that permit authorized access to information and services that are available to the PSAP through the Emergency Services IP Network. It also allows other authorized agencies and contractors who need information or services that reside in the PSAP to access such data or services. These interfaces are concerned primarily with information and services pertaining to a specific call or event.		
Information access by the PSAP		
A variety of databases may be available to the PSAP. These databases are characterized by being associated with some key which is obtained directly or indirectly from the call, and where the response of the database is to return information that it associates with that key. An example would be retrieval of information associated with a location (c.f. Requirement 4.2.11)		
Services access by the PSAP		
A variety of services may be available to the PSAP. These services are characterized by actions to be taken on the PSAPs behalf, initiated by request of the PSAP, as well as notification of asynchronous events by the service to the PSAP. An example would be accessing a logging service to play back previously recorded media.		
Information Access from the PSAP		
Other authorized agencies or contractors may need access to data that resides in the PSAP. As with database access by the PSAP, a request may include a "key" and the response is to return information associated with the key. Other data, e.g. administrative information, may also be accessed.		
Service access from the PSAP		
A PSAP may provide a service to other agencies or contractors connected to the Emergency Services IP Network. As with services provided to the PSAP, actions will be taken upon request of the external entity. The PSAP may also provide asynchronous event notifications.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
<p>Note: This description does not imply that there is a fundamental difference between Databases and Services. It is often the case that side effects occur resulting from a database query, e.g. invoking additional services. It is also the case that databases are often accessed and updated in performing a service. The distinction here is merely to make sure all requirements are captured.</p>	<p>[12a]</p>	
<p>There are a wide variety of services and databases that may be made available to PSAPs which are not specifiable by NENA. Thus, while we present requirements here, we recognize that if a PSAP desires to use a database or service defined elsewhere, it should be permitted to do so without involvement of any layer or adapter that forces the service or database to fit a single model. PSAPs should use these requirements as a guide to evaluate such services to see how compatible they may be with other, NENA-defined, databases and services.</p>		
<p>The Emergency Services IP Network may be shared with many public safety agencies and contractors, and as such, we must define our interfaces to conform to standards agreed upon among all such agencies.</p>		
<p>4.2.1 Information Access and Services Awareness</p>		
<p>For a database or service to be used, it must be known to the PSAP (for databases or services accessed by the PSAP) or advertised by it (for databases or services it offers to the network). Services are provided by a domain, which we define here as a set of addressable entities under common administrative control (which might be the local Emergency Services IP Network itself, or a service provider within it. The PSAP should be able to discover services and become aware of new services as they are introduced as well as the removal existing services.</p>		
<p>ServiceBasic 0100-0100 Databases and services shall have globally unique identifiers</p>		<p>[12a]</p>



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
ServiceBasic 0200-0100 Mechanisms for discovery of, and connection to services which MAY be used by services provided shall be specified.	[12a]	[12a]
ServiceBasic 0300-0100 Where there are multiple instances of the same service (same id), there must be a mechanism to identify each instance.		
ServiceBasic 0400-0100 There shall be a mechanism by which an entity can determine if a particular database or service is provided, and if so, how to contact the database or service within a domain.		
ServiceBasic 0500-0100 There should be a mechanism by which multiple service providers providing the same service but differentiated by a qualifier can be selected based on a specific value of the qualifier.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
ServiceBasic 0600-0100 It should be possible to have the exact same service offered by multiple, competing service providers.	[12a]	[12a]
ServiceBasic 0700-0100 PSAPs must always opt-in to services provided on the network. No services shall be provided which a PSAP does not explicitly request, regardless of whether or not the service is free or has a cost associated with it		
ServiceBasic 0800-0100 Services must inform PSAPs of its availability or non availability, both planned and unplanned.		
ServiceBasic 0800-0100 Provisioning of new services to a PSAP must be graceful and not require non-related services to be affected		
4.2.2 Incidents		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
<p>In order that multiple databases and services may be utilized by multiple agencies in handling of calls, there needs to be ways to relate elements in some way so that correlations are possible. We use the following definitions:</p> <p>Agency: an organization that is a client of a database or service.</p> <p>Agent: a person employed by or contracted by an agency.</p> <p>Call Request: a single communication to a PSAP that results in a defined action by a call taker. A call does not have to be a literal phone call. It could be an Instant message, a SMS text message, an Automatic Crash Alert, etc.</p> <p>Incident: a defined public safety event that incurs a response within the domain of a PSAP. Examples include a traffic accident (including subsequent secondary crashes), a hazardous material spill, etc. Multiple Call Requests may be associated with an Incident</p> <p>Interagency Incident: One or more incidents that span multiple PSAPs and involve multiple response agencies. A disaster involving a wide region is an example, but any incident involving more than one primary PSAP is an Interagency Incident. Multiple incidents within a PSAP may be associated with an Interagency Incident.</p> <p>The life cycle of a Call Request includes: call origination, call abandonment or completion, call duration, call clearing, and post-call processing of indefinite duration.</p>	<p>[12a]</p>	
<p>Incident.0100-0100 It shall be possible to uniquely identify an agency within the national Emergency Services IP Network</p>		
<p>Incident.0200-0100 It shall be possible to uniquely identify an agent within an agency</p>		<p>[12a]</p>
<p>Incident.0300-0100 It shall be possible to uniquely identify a Call Request throughout its life cycle, across multiple transfers of the call among agencies</p>		
<p>Incident.0400-0100 A PSAP or a service on the ESInet may declare an Incident</p>		
<p>Incident.0500-0100 It shall be possible to uniquely identify an Incident throughout its life cycle.</p>		
<p>Incident.0600-0100 It shall be possible to associate multiple calls with an Incident</p>		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Incident 0700-0100 Incidents may be declared to be within a hierarchy of incidents, where one incident has a number of subsidiary incidents associated with it. There can be an unlimited number of levels.	[12a]	[12a]
Incident.0800-0100 All databases and services shall make use of Agent, Agency, Call Request, Incident and Interagency Incident identifiers to uniquely associate data and events with the proper identifiers.		
Incident.0900-0100 Wherever practical, database entries, accesses and updates, as well as service invocations and events shall be correlated to the appropriate call, incident or interagency incident as appropriate		
Incident 1000-0100 It shall be possible to interleave messages for multiple active incidents in any order.		
Incident 1100-0100 Call Requests and Incidents can be active or inactive at a specific agency. An active Call Request corresponds to an emergency service request undergoing processing by a call-taker.		
Incident 1200-0100 A Call Request becomes inactive at the agency when it is declared as such by the agency, possibly causing disengagement from associated services.		
4.2.3 Bridge Services		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Bridge 0100-0100 Bridge services may be provided as a service on the ESInet, or may be provided internal to the PSAP.	[12a]	[12a]
Bridge 0200-0100 All participants in the bridge must have access to the call identifier of the original call.		
Bridge 0300-0100 Information gathered by one agency on the call request must be available to other agencies being bridged. It must be possible for the bridged agency to be made aware such information exists.		
Bridge 0400-0100 Any agency on the call must be made aware of any other agencies (or external participant) bridged to the call.		
Bridge 0500-0100 Provision for bridging agencies that are only accessible via Selective Router or PSTN must be defined		
Bridge 0600-0100 An i3 PSAP must be able to transfer or bridge a call to or from any PSAP, including internationally, with all data that accompanied the call (e.g. location)		
Bridge 0700-0100 The call-taker must be able to control what the caller hears while bridge/transfer operations are completed.		
4.2.4 Information Discrepancy Service		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
<p>In any service or database there is the potential for a discrepancy noted by the user of the data or service. This includes a misroute of a Call Request. An information discrepancy service allows this discrepancy to be sent to the appropriate administrative agency for correction. The agency then may return a tracking ticket and notify the using agency of the disposition.</p>	<p>[12a]</p>	
<p>Discrepancy 0100-0100 Databases and services should include a mechanism for an agency using the database or service to report any discrepancy it noted, specifically inclusive of misrouted information.</p>		<p>[12a]</p>
<p>Discrepancy 0200-0100 A method for including free form text must be included in a discrepancy report.</p>		<p>[12a]</p>
<p>Discrepancy 0300-0100 Once the receiving agency receives the information discrepancy report it shall return an identifier for the discrepancy to the using agency.</p>		<p>[12a]</p>
<p>Discrepancy 0400-0100 Once the information discrepancy is resolved by the managing agency a status report shall be sent to the using agency.</p>		
<p>Discrepancy 0500-0100 i3 shall define a standardized mechanism for this purpose which should be used by databases and services that do not have a valid reason for using another method</p>		<p>[12a]</p>
<p>Discrepancy 0600-0100 Discrepancy reports and status reports should have at least one free text field</p>		
<p>4.2.5 Report and Status Services</p>		
<p>Report 0100-0100 Where a response to a request may take significant time to complete, databases and services should provide status reporting mechanisms to allow the requestor to determine the status of an outstanding request</p>		
<p>Report 0200-0100 Where appropriate, services should provide mechanisms to request historical reports</p>		
<p>Report 0300-0100 Where appropriate, services should provide mechanisms to request configuration reports</p>	<p>[12a]</p>	



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Report 0400-0100 Where appropriate, services should provide mechanisms to request reports by type of incident, location of incident (Geo or civic) and date range to allow authorities to map incidents by geographic area.	[12a]	[12a]
4.2.6 Network Requirements		
The Emergency Services IP Network is expected to be an internetwork (network of networks) of IP networks joined by routers. Logically, the local Emergency Services IP Network joins all public safety agencies in a jurisdiction, and that local network is interconnected, perhaps to neighboring jurisdictions. Physically, the Emergency Services IP Network will consist of several networks, with different layer 2 mechanisms, including wireline, wireless, government owned facilities, leased private facilities, virtual private networks, etc. The network should be managed to be as secure as practical. However, no element of the network should assume that it is secure. The network between the PSAP and the ESInet will be a private or virtual private network based upon TCP/IP. It will have scalable bandwidth to support new enhanced services. The network must be robust to support all categories of media, including text, graphics and video based upon the applications that are supported. The Emergency Services Network is connected to the Internet through firewalls.		
Network.0100-0100 The Network connectivity between the PSAP and the ESInet shall be a private or virtual private network based upon TCP/IP.		
Network.0200-0100 The protocols and the corresponding networks shall be capable of supporting the transmission of images, video, high resolution graphics, non real time voice, and other capabilities.		
Network.0300-0100 Connections between the PSAP and ESInet shall be secured TCP/IP connections such that advanced authorization, authentication and security features can be implemented.		
Network.0400-0100 DiffServ Code Points to be used for PSAP needs shall be specified		
Network.0500-0100 NAT may be required in some jurisdictions between the Emergency Services IP Network and the Internet, so all services intending to use Internet connections must assume NAT.		
Network.0600-0100 i3 defined service applications must be capable of operating on IPv4 and IPv6 network infrastructures.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
4.2.7 Protocol Requirements	[12a]	
The protocols between the PSAP and ESInet will be bi-directional to support the new services that will be implemented. The protocols should allow end points to discover each other. Where standards exist, they should be used instead of special-purpose protocol specifications, wherever possible. This does not preclude 3GPP, ESIF or NENA-specified application protocol interfaces for services and data exchanges.		
Protocol.0100-0100 Domain names (DNS) should be used in preference to IP addresses		
Protocol.0200-0100 Application interfaces should have versions, and versions should be negotiable.		
Protocol.0300-0100 Mechanisms used in failure and recovery situations shall be capable of being exercised to ensure they are operating properly.		
Protocol.0400-0100 Services should be designed such that making a service available or unavailable shall not affect any other service not dependent on it. This may be an obligation on both the client and the server.		
Protocol 0500-0100 Reliable services should be designed such that failure of a server shall not affect the service.		
Protocol.0600-0100 Redundancy mechanism specification of a service must include what granularity of transaction integrity is provided. Database access systems might use two phase commit with rollback. SIP might use a paradigm where calls that are signaled complete stay up, calls that initiate after failure go through, calls in the middle of signaling establishment fail and must be retried.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
4.2.8 Security/Privacy	[12a]	
<p>Databases and Services should require authentication before use. Authentication may be by agency, for databases and services that are not specific to a person within the agency, or by person, which are specific to a person. Authentication requires credentials. Authorization specifies what actions or access is permitted and is subject to policy of both ends. Integrity protection insures messages sent across the network cannot be forged or modified without detection. Privacy prohibits reading messages when not authorized to do so.</p> <p>Databases containing sensitive information and Services which provide sensitive functionality require suitable authentication and access restrictions for use. Authentication may take several forms and may apply on a personal level or agency level. Person-based authentication schemes may incorporate such mechanisms as passwords, smartcards or tokens. Agency based authentication schemes may employ such mechanisms as system-to-system authentication via x.509 digital certificates.</p> <p>Access rules and restrictions must be employed by sensitive databases and services to ensure that actions taken within the system are limited to only authorized personnel and agencies. It is the responsibility of database and service operators to ensure that personnel and/or agencies have been authenticated and access controls are applied to a level of satisfaction appropriate to the sensitivity of the database or service.</p>		
<p>Security.0100-0100 Elements connected to the ESInet which provide access to sensitive data or services shall require users and/or their agencies to be authenticated prior to being granted access to such element.</p>		
<p>Security 0200-0100 Authentication shall be by agency or by person, depending on the nature of the database or service provided. Person authentication is preferred in order to provide accountability for actions taken by personnel in the network.</p>		
<p>Security 0300-0100 The specific authentication mechanisms for the Emergency Services IP Network should be that agreed to among public safety agencies. The specific credentialing mechanisms employed should be as agreed to.</p>		
<p>Security 0400-0100 i3 shall define credentialing mechanisms for agencies and employees/contractors within those agencies</p>		
<p>Security 0500-0100 Credentials issued per Security 0400-0100 should be used for database access and service authentication</p>		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Security 0600-0100 Person-based authentication mechanisms shall be provided to support password-only (weak) or two-factor (strong) user authentication between a PSAP CPE and ESInet based on the configuration of the ESInet.	[12a]	[12a]
Security 0700-0200 Password based authentication mechanisms shall protect the password such that it is possible for the user to prove knowledge of the password without transmitting the password.		[12a]
Security 0800-0100 It must be possible for security-sensitive actions taken within the network to be associated with a person or agency in a manner that provides non-repudiation by the responsible party. Such actions must be historically traceable back to the responsible party in a manner that provides non-repudiation by the responsible party of the accuracy of the historical information.		
Security 0900-0100 Proxy authentication should be used so that "Single Sign On" can be achieved.		
Security 1000-0100 All sensitive communications over the Emergency Services IP Network that directly relate to emergency databases and services shall be protected by suitable Integrity Protection mechanisms.		
Security 1100-0100 All sensitive communications over the Emergency Services IP Network that directly relate to emergency databases and services shall be protected by suitable Privacy mechanisms.		
Security 1200-0100 The mechanisms chosen for Security requirements above shall use multiagency standards wherever possible		
Security 2100-0100 i3 implementations should adhere to existing national standards and best practices in security.		
Security 2100-0200 Signaling and control elements of i3 implementations should conform to the standards and practices set forth in Generic Signaling and Control Plane Security Requirements for Evolving Networks Standard [American National Standard ATIS-1000007].		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Security 2100-0300 Management systems and network elements of i3 implementations should conform to the standards and practices set forth in Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane [American National Standard T1.276-2003]	[12a]	
4.2.9 Maintenance		
External interfaces between the PSAP and databases and services should incorporate best practices to maintain maximum system availability. Hardware elements should be able to come into service and go out of service without impacting the overall service availability.		
Maintenance 0100-0100 Mechanisms in protocols and services must incorporate methods for each end to monitor the health of the other. Specific services may be designated as non critical and thus exempt from this requirement		
Maintenance 0200-0100 Any device with an external interface, or any database or service available via an external interface shall be capable of being brought into or out of service without affecting other databases or services not dependent on it.		
Maintenance 0300-0100 Hardware elements of high availability services shall be capable of being brought into or out of service without affecting the overall service availability		
Maintenance 0400-0100 A mechanism shall be defined to advise management and/or users of impending maintenance service activities for non-high availability services.		
Maintenance 0500-0100 Integrity and authenticity of data in databases accessible to any party must be capable of being verified by that party		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Maintenance 0600-0100 Any device or database service must be capable of having its software upgraded without affecting the availability of the device or service.	[12a]	[12a] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
4.2.10 Additional Data		
Information will be available to PSAPs that is not necessarily delivered with the call, but is associated with the location, caller or call.		
AdditionalData 0100-0100 Mechanisms for providing additional data must be made available to the PSAP		
AdditionalData 0200-0100 PSAPs must request such data, either at the time it wishes to get the data, or as part of service enrollment		
AdditionalData 0300-0100 Additional Data may be located within the Emergency Services IP Network, or in public networks		
AdditionalData 0400-0100 Mechanisms must be provided to require authentication prior to being authorized to access additional data		
AdditionalData 0500-0100 Mechanisms must be provided to protect additional data privacy.		
AdditionalData 0600-0100 Where additional data is not stored in the PSAP, and the data is relatively static, mechanisms must be provided that allow a PSAP to cache the data for fast retrieval under times of system stress (such as disasters).		[REDACTED] [12a] [REDACTED]
AdditionalData 0700-0100 Processes must be established to standardize representation of additional data, which must involve the owners/creators of that data		[REDACTED] [12a]



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
AdditionalData 0800-0100 Information provided on the call must be sufficient to locate information associated with the location, caller or call.	[12a]	
AdditionalData 0900-0100 Additional Data may be provided by other agencies or services in the Emergency Services IP Network		
4.2.11 Additional Data associated with a location		[12a]
AdditionalLocationData 0100-0100 Distinction must be made between data associated with a building or campus and a tenant of such a building or tenant. Each source may have different additional data		
AdditionalLocationData 0200-0100 There must be a mechanism to determine the tenant from the building owner/manager for a call in order to correctly query for tenant specific additional data		
4.2.12 Additional Data associated with a caller		
AdditionalCallerData 0100-0100 Mechanisms must be provided to support additional data associated with the Address of Record of the caller		
AdditionalCallerData 0200-0100 Information associated with a caller must be opt-in by the caller only		
AdditionalCallerData 0300-0100 Information associated with a caller may include Private Health Information as defined in the HIPAA and mechanisms must be provided to protect that data according to that rule <ref, abbb>		
4.2.13 Additional Data associated with a call		
AdditionalCallData 0100-0100 Mechanisms must be provided to support additional data associated with the call		
4.2.14 Other		
OtherData 0100-0100 Mechanisms must be provided to implement [12a] from call takers (PSAP policy controller).		
OtherData 0200-0100 Mechanisms must be provided to support external services not directly tied to a call		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
4.3 Connections to Downstream Systems	[12a]	
4.3.1 Choosing a Responder		[12a]
ChooseResponder 0100-0100 The i3 PSAP shall be capable of associating an indefinite number of responders with a location		
ChooseResponder 0200-0100 The service boundaries of responders shall be specifiable in polygon and/or civic address forms.		
ChooseResponder 0300-0100 There shall be no assumptions made concerning alignment of responder service boundaries to PSAP service boundaries, any political boundary or the service boundary of any other responder.		
ChooseResponder 0400-0100 Responders shall be classified into a list maintained by NENA. Examples of classifications would be police, fire, EMS, poison control, animal control		
ChooseResponder 0500-0100 It shall be possible for more than one responder to provide the same classification of service to the same location.		
ChooseResponder 0600-0100 It should be possible to have specialties within a classification based on specific capabilities of a responder		
ChooseResponder 0700-0100 The PSAP shall be able to determine the Display Name (English Language Translation), classification, for a responder		
ChooseResponder 0800-0100 The i3 PSAP shall be capable of bridging/transferring a call to any responder(s) associated with the call without placing the call requester on hold		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
ChooseResponder 0900-0100 The i3 PSAP shall be capable of bridging/transferring a call to any PSTN or VoIP address	[12a]	
ChooseResponder 1000-0100 For responders that are connected to the PSAP via VoIP, all information received with the call shall be sent with the transfer/bridge		
ChooseResponder 1100-0100 Any information entered/created by the call taker shall be made available to the responder.		[12a]
ChooseResponder 1200-0100 For responders that are connected to the PSAP via the Selective Router introduction of i3 must not cause them to lose functionality they have now.		
ChooseResponder 1300-0100 Responders must have access (subject to appropriate authentication and access controls) to data associated with a location, caller or call.		
ChooseResponder 1400-0100 Responder selection shall be capable of working independently of the type of originating network. This implies the i3 responder selection mechanisms should work on calls to the PSAP arriving via a selective router. This requirement does not preclude an implementation from also supporting ALI based ESN selection of responders.		
ChooseResponder 1500-0100 Any media stream (voice, video, text or image) received by the PSAP shall be bridgeable/forwardable to responders if it is capable of receiving them.		
ChooseResponder 1600-0100 Call takers shall be able to communicate with dispatchers of any responder via voice, video or text if the responder is capable of it.		
4.3.2 Other disposition of calls		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
OtherDisposition 0100-0100 A PSAP must be able to control disposition of calls not answered by a call taker. Such dispositions include queuing a call, returning a busy indication, connecting the call to an Interactive Voice/Text Response Unit, or routing the call to an alternate PSAP.	[12a]	[12a]
OtherDisposition 0200-0100 Treatment of calls as per OtherDisposition 0100-0100 may be dependent on the media request of the caller		
OtherDisposition 0300-0100 PSAPs shall be notified of abandoned calls, and be able to obtain location and call back information included for such calls		
OtherDisposition 0400-0100 Sessions to PSAPs shall have mechanisms to determine if a call is dropped without normal termination messaging		
OtherDisposition 0500-0100 PSAPs shall be able to accept non-emergency calls placed to, for example 3-1-1		
OtherDisposition 0600-0100 Non emergency calls shall be capable of being differentiated from emergency calls		
OtherDisposition 0700-0100 PSAPs shall have the capability to apply different call treatments (per OtherDisposition 0100-0100) to non-emergency calls, specifically, where queuing services are provided, non-emergency calls may require separate queues.		
OtherDisposition 0800-0100 PSAPs shall be provided mechanisms to deal with large volumes of fraudulent calls as part of a deliberate attack on the PSAP.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
OtherDisposition 0900-0100 Mechanisms shall be provided to recognize non-emergency calls marked with priority (for example, the SIP Resource Priority Header), and provide different disposition of such calls from unmarked calls	[12a]	[12a]
4.3.3 Computer Aided Dispatch		
CAD 0100-0100 Support for existing NENA CAD interfaces must be provided		
CAD 0200-0100 A new CAD interface providing facilities commensurate with the data and signaling requirements presented herein shall be specified.		
4.4 Connections to Local, Regional, State and Federal Authorities and peer connections		
Exterior 0100-0100 It shall be possible for authorities superior to a PSAP to have visibility into events occurring within the PSAP, such as unusual call volume, significant failures, etc.		
Exterior 0200-0100 It shall be possible for Incident information as defined in Section 4.2.2 to be made available to higher level authorities.		
Exterior 0300-0101 0100 It shall be possible for a PSAP to provide or receive Incident information as defined above to/from other PSAPs		
Exterior 0400-0100 Services available from other authorities (e.g. [12a]) should be available to PSAPs on the Emergency Services IP Network as any other service described herein		
4.4.1 Disaster Management		
Disaster 0100-0100 PSAPs shall have interfaces to EPAD (and similar event notification systems) to both accept and generate events.		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Disaster 0200-0100 Routing of calls in a disaster shall be one of the cases of alternate routing detailed in Section 4.1.8	[12a]	
4.4.2 PSAP Backup/Failover		
BackUp/Failover 0100-0100 When a PSAP fails, calls intended to route to it shall route to one or more designated PSAP(s)		
BackUp/Failover 0200-0100 There must be a mechanism to allow PSAPs to designate its backup PSAP(s), and such PSAP(s) must agree to provide backup service		
BackUp/Failover 0300-0100 Calls arriving from a failed PSAP must be identifiable by the backup PSAP as being failover calls	[12a]	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
BackUp/Failover 0400-0100 When a failed PSAP with backup arrangements activated comes back in service, a graceful transition to the revived PSAP must occur		
BackUp/Failover 0500-0100 It must be possible to have a redundant (duplicate) PSAP that is capable of immediately taking over responsibility for a failed PSAP		
BackUp/Failover 0600-0100 Security mechanisms designed to assure identity of PSAPs must work reasonably well when backup PSAPs are processing calls for a failed PSAP.		
BackUp/Failover 0700-0100 It must be possible for the backup PSAP to transfer calls and data associated with calls to any of the dispatch functions the failed PSAP could. Capabilities at the backup PSAP may limit the functionality the backup can provide.		
BackUp/Failover 0800-0100 No assumptions should be made on where the backup PSAP is located, Specifically, the backup PSAP may not be on the same Emergency Services IP Network as the failed PSAP.		
4.5 Other		



NENA 08-751 Section 4 Functional Requirement	Compliance	Comments
Other 0100-0100 An Intra/Inter PSAP Instant Messaging system shall be specified with connections to similar systems available to responder dispatcher/management	[12a]	[12a]
Other 0200-0100 There shall be no single point of failure in conforming i3 implementations. Specific services could be designated as non critical and thus exempt from this requirement		
Other 0300-0100 Each subsystem in conforming i3 implementations shall be designed such that the system survives major disruption including disaster, deliberate attack, and massive element failure.		
Other 0400-0100 Mechanisms to mitigate "Distributed Denial of Service" attacks or similar malicious situations shall be specified		
Other 0500-0100 All databases used by conforming i3 implementations shall support manual query (under PSAP policy control and within any local or state law) to the call taker or management systems.		
Other 0600-0100 A service must be defined to log all media and all events with timestamps such that a complete picture of a call can be reconstructed from the log after the call.		[12a]
Other 0700-0100 Mechanisms to test each element and complete call chains from caller end device to internal PSAP systems without interfering with real emergency calls shall be specified		
Other 0800-0100 A mechanism must be specified to achieve synchronized time across multiple devices, services and agencies.		



7.2.15. Basic Call Processing Enhancements [RFP 6.2.15]

This section identifies the basic call processing enhancements necessary to ensure that a 9-1-1 call is always delivered to a PSAP somewhere within the system should the primary, or even alternate, PSAP be unavailable. These requirements are not intended to dictate any "state-full" implementation of SIP, but the BIDDER may decide that this affords the degree of protection herein required.

7.2.15.1. LNG(s) to ESRP – [RFP 6.2.15.1]

Should any response other than a "200 OK" message be received from the ESRP, the LNG will re-attempt the call to the other ESRP(s) within the ESInet. If, after re-attempting the call, a "200 OK" or a "486 Busy Here" message is still not received for the call, an alarm shall be raised and maintenance personnel dispatched immediately to investigate the root cause. The LNG will then attempt to route the call to the PSTN Gateway (if provided in the BIDDERS solution) as follows:

- *(Preferred) Attempt to connect the call via a PSTN gateway by using the 10-digit PSTN number associated with the Primary PSAP unless it is in the "Abandoned" state in which case the 10-digit PSTN number associated with the Backup shall be used. If the Backup is also in an "Abandoned" state the "Default" 10-digit PSTN number shall be used; or*
- *Provide, or cause to be provided, an announcement back to the 9-1-1 caller which informs them of the 10-digit PSTN number that can be used to reattempt the call (Primary, Backup or Default depending upon "Abandonment" state).*

This feature shall be settable on a per PSAP basis with a default setting of OFF.

Regardless of the approach taken, an alarm shall be raised, indicating that a 9-1-1 call could not be terminated via the ESInet and maintenance personnel shall be immediately engaged to determine/confirm the reason.

We offer a PSTN gateway as part of our solution. Therefore, we are compliant with the preferred method of attempting to connect the call via the PSTN gateway. Ultimately, if both the primary and backup PSAPs are unavailable, default routing will be used to connect the call. [REDACTED]

[12a] [REDACTED] A log of the default routing action will be generated and acted upon to resolve the issue.

7.2.15.2. INTENTIONALLY OMITTED

7.2.15.3. ESRP PSTN Gateway Routing – [RFP 6.2.15.3]

In the event that an ESRP cannot deliver a call to a PSAP (Primary, Backup, Default) served by the ESInet, the ESRP shall;

- *(Preferred) Attempt to connect the call via a PSTN gateway by using the 10-digit PSTN number associated with the Primary PSAP unless it is in the "Abandoned" state in which case the 10-digit PSTN number associated with the Backup shall be used. If the Backup is also in an "Abandoned" state the "Default" 10-digit PSTN number shall be used; or*
- *Provide, or cause to be provided, an announcement back to the 9-1-1 caller which informs them of the 10-digit PSTN number that can be used to reattempt the call (Primary, Backup or Default depending upon "Abandonment" state).*

This feature shall be settable on a per PSAP basis with a default setting of OFF.

Regardless of the approach taken, an alarm shall be raised, indicating that a 9-1-1 call could not be terminated via the ESInet and maintenance personnel shall be immediately engaged to determine/confirm the reason.

We offer a PSTN gateway as part of our solution. Therefore, we are compliant with the preferred method of attempting to connect the call via the PSTN gateway. Ultimately, if both the primary and backup PSAPs are unavailable, default routing will be used to connect the call. [REDACTED]

[12a] [REDACTED] A log of the default routing action will be generated and acted upon to resolve the issue.



7.2.16. INTENTIONALLY OMITTED

7.2.17. INTENTIONALLY OMITTED

7.2.18. ESInet Support for Legacy (CAMA) PSAPs – Legacy PSAP Gateway [RFP 6.2.18]

Despite the ESInet being an all IP network, some of the PSAPs may remain Analog for years to come. The interface mechanism will remain CAMA trunks, which enable the signaling to include an MF ANI field that may consist of 7, 8, 10 or 20 ANI (MF) digits. Further, analog and RFAI PSAPs will still perform an ALI query to obtain ALI information from the ALI database, which will remain part of the NG9-1-1 system until fully supplanted with the LIS function or BIDDER innovation.

As MIL has allowed for deviations from the NENA architecture (e.g., location of the LNG LIF in the ESRP) and an i3 compliant LIS may be unavailable in the originating network for some time to come. The requirements in Section 7.2 Legacy PSAP Gateway, of NENA 08-003 will need to be modified to “fit” the BIDDERS proposed solution. Further, as it is highly unlikely that MIL would ever work with anyone other than the successful BIDDER to enhance LPG functionality, only the external interfaces need be compliant with the i3 model. That is, how the PIF, NIF and LIF communicate with each other is left to the BIDDERS discretion.

As required, NENA i3-compliant LPGs will be deployed on the ESInet to facilitate initial call delivery and call transfers, as well as ALI transactions, from the ESInet to legacy and RFAI PSAPs. These gateways are similar in capability to the LNG/LSRG in terms of protocol conversion (SIP-to-TDM). They also offer functions that help the PSAP retrieve ALI information – even if it is delivered in the form of a PIDF-LO – to facilitate both inter- and intra-ESInet call transfers by using the ECRF. For example, a PSAP that normally signals *11 to the legacy SR for transferring a call to the police agency associated with that particular ALI would do the same if it receives the call from an LPG. The difference is that, as opposed to a tabular lookup on a legacy SR, *11 would be translated to a service URN by the LPG for the police entity [12a] and in turn invoke the “police” GIS layer on the ECRF to provide a destination URI based on the caller’s PIDF-LO. All these ESInet transactions are facilitated by the LPG (NIF and LIF, respectively) on behalf of the legacy PSAP. All functions outlined for both the NENA i3 LNG and the proposed LSRG for transition and interaction with legacy SRs are supported within this proposed platform.

While the BIDDER should attempt to comply with the NENA LPG requirements, only the following shall be considered Mandatory.

7.2.18.1. SIP Interface – [RFP 6.2.18.1]

The LPG shall support a SIP interface towards the ESInet as identified within NENA 08-003.

TCS’ LPG supports a SIP interface with the ESInet, in compliance with NENA 08-003.

7.2.18.2. CAMA Interface – [RFP 6.2.18.2]

The LPG shall support a CAMA interface towards the PSAP CPE that is compliant with the requirements of NENA 08-003.

TCS’ LPG supports a CAMA interface with the PSAP CPE in compliance with NENA 08-003.

7.2.18.3. ALI Interface – [RFP 6.2.18.3]

BIDDER shall comply with the ALI interface requirements identified in NENA 08-003.



TCS's ALI interface complies with the applicable requirements identified in NENA 08-003.

7.2.18.4. Support for Star Codes – [RFP 6.2.18.4]

The LNG (and ESRP) shall support the use of star codes as specified within NENA 08-003; with the modification that star codes within Washington State are 3-digits (as opposed to the 2-digits identified in NENA 08-003). There are approximately 200 different star codes in use within the existing ESInet. The listing of Star Codes currently in use will be provided to the successful BIDDER after the contract has been signed.

The proposed solution supports the necessary extra digits or codes necessary to automatically dial a number and complete a call. The solution supports star code speed dials through the ESInet, and we will work with Washington to provision the star codes currently in use.

7.2.19. ESInet Connectivity – [RFP 6.2.19]

7.2.19.1. ESInet PSAP – [RFP 6.2.19.1]

Currently the only ESInet-PSAP connectivity mechanism is via traditional Telephone Company T1 lines, by using what is generally referred to as "IP over TDM". Further, while affording IP-based connectivity, they are still limited to transmission rates of 1.544 Mbps, although "bonding" allows higher transmission rates. With the advent of true NG9-1-1 and the transmission of multi-media (e.g., video calls), T1 connectivity may not provide sufficient capacity for a PSAP's requirements and bonding may not be economically viable in relation to other connectivity mechanisms (e.g. what is generally referred to as Ethernet Local Access (ELA)).

BIDDER shall identify the connectivity mechanisms that will be supported by their proposed solution. It is understood that some PSAPs may not have a choice in the connectivity mechanism (i.e., only T1 connectivity exists). Accordingly BIDDERS should use Attachment G and identify what connectivity mechanisms can be made available at each location.

The TCS [12a] ESInet supports scalable IP connectivity. We understand that current T1 connectivity may only be economically viable in certain locations, [12a] Wireless connectivity is also available for most sites, but is not priced as part of our response.

7.2.19.2. ESInet-Originating Network Connectivity – [RFP 6.2.19.2]

Currently most Originating Network Emergency Service circuits (trunks) terminate upon CenturyLink Network Aggregation Points (NGAPs) located in Seattle, Tacoma, Portland, Spokane and Yakima, although some circuits terminate directly upon the LNGs themselves and are located in Seattle, Tukwila, Liberty Lake and Yakima. Accordingly some BIDDERS may have to work with CenturyLink and the direct connect Service Providers to rehome the circuits to new LNGs either in the same locations or in new locations.

BIDDER shall make the necessary arrangements and provide the associated functions (i.e., LNGs) to interconnect to the Originating Network via the existing Emergency Service circuits to the ESInet. A detailed inventory of which will be provided to BIDDERS attending the pre-bid conference and completing the NDA (Attachment B).

We will work with the CSPs to rehome all necessary circuits to our ingress points for both TDM (LNG/LSRG) and SBC (IP) connections.

7.2.20. INTENTIONALLY OMITTED

7.2.21. Logging and Reporting Functions [RFP 6.2.21]

In addition to the specific logging and reporting functions identified in other sections of this document, the following general requirements and additions shall also apply.



7.2.21.1. General – [RFP 6.2.21.1]

Extensive logging of the NG9-1-1 ESInet transactions and operations is required. All log entries shall be accurately time stamped in PTZ time. Only authorized software processes shall have write access to log files. Log files shall be read-only to all other processes and users. Because logs may be subpoenaed and may otherwise become the source of information in legal proceedings, the log systems shall be designed, proposed, and operated with legal defensibility of log information taken into careful account.

Because of the redundant and diverse nature of the ESInet, safely and securely consolidating all log information into centralized log stores is an important consideration. These consolidated log stores provide management information system (MIS) functions rapid and easy access of the log data. The MIS system generates tabular and summary statistical reports from the log data.

The NG9-1-1 ESInet logs shall fall into two (2) categories: transactional logs, which record the routine handling of each and every call by various system components; and operational logs, which record status of configuration changes, operator access and interventions, or exceptional events in the operation of the logged component, process, or instance.

TCS' partner, [12a], provides an i3 Meta logger that is able to be subscribed to by functional elements in the ESInet for transactional log distribution. Operational logs are independent of the ESInet and are not part of the i3 standard. Therefore, the ability to ingest and capture these logs is not a function of the logger, nor is it defined by i3; rather, it is a function of the source systems supporting the export of the logs and the intake system that has a legend for interpreting the logs. [12a] can provide multiple paths for ingestion and will develop necessary proprietary interpreters for the operational logs, but [12a] is not able to make logging available in systems that do not support operational logging.

Therefore, as a supplement to the [12a] meta logger, TCS will provide access to the operational logs as identified here and elsewhere using internal logging processes. Our systems already maintain extensive logs with operational details, and we will summarize these log events in our central warehouse to fulfill the logging requirements.

7.2.21.2. ESInet Element Logs – [RFP 6.2.21.2]

All elements in the call flow such as the LNG, BCF(s), ESRP, PRF, ECRF, LVF, PGM and ALI database shall maintain local (dedicated to that instance) "raw" transactional logs and operational logs. These logs shall contain, at a minimum, a process instance identifier, and the date and time-stamped record (PTZ) of each SIP, LoST or ALI message processed. Local raw logs shall be maintained for at least thirty (30) days, during which time they shall have been copied to consolidated raw log files for storage for seven (7) or more years.

7.2.21.3. ESInet Element Log Consolidation – [RFP 6.2.21.3]

Local transactional logs shall be consolidated into a single consolidated raw transactional file. Local raw operational logs shall be consolidated into a single raw operational file. These consolidations shall be performed incrementally via an automated process at real-time or at regular intervals, [12a].

We maintain a [12a] for the capture and dissemination of operational logging data. Our process is built on top of the operational intelligence engine provided by [12a] provides the industry-leading software to consolidate and index any log and machine data, including structured, unstructured, and complex multiline application logs. [12a] continuously consolidates logs, and we will ensure the process is incrementally active within [12a].

Similarly, [12a] employs an analytics system to store raw data to their system, which will be done on an automated basis.



7.2.21.4. Log File Redundancy – [RFP 6.2.21.4]

At least one copy of the consolidated raw log files shall be maintained at a minimum of two geographically diverse data centers. The consolidation process should alternate between the two sites, and be equipped with sanity checks such that if a failure of the consolidation process fails and destroys, as through a software defect, one of the consolidated raw log files, then that process will halt, the original final left unchanged and an alarm will be raised, or similar safeguards will protect the undamaged consolidated log file(s). BIDDERS may propose alternate mechanisms to insure the integrity and security of the consolidated log files. BIDDERS shall *thoroughly explain the safeguards against the loss of consolidated raw log data.*

[12a] does not perform log aggregation at the collection point. Rather, aggregation and reporting is done in real time with a query of the [12a] analytics system. [12a] stores the raw data directly into our analytics platform and provides interfaces to aggregate and spill data in response to queries performed against the analytics system.

Operational logs, as consolidated by [12a], will reside at our geographically redundant CLCs. All raw log files will be maintained on the primary call service systems, then collected from there and consolidated into [12a]k. TCS [12a] system is a georedundant platform, fully protected from data loss by implementing data storage on highly resilient and redundant storage systems. All raw data is collected from primary systems into the [12a] and replicated to both georedundant sites. If there is a temporary failure in the replication, it is queued up and replicated when the georedundant site becomes available.

7.2.21.5. Consolidated Log File Retention – [RFP 6.2.21.5]

Consolidated raw transactional and consolidated operational log files shall be maintained for a minimum of seven (7) years.

We will maintain raw transactional and consolidated operational log files for a minimum of seven years.

7.2.21.6. Consolidated Raw Transactional Logs: Database – [RFP 6.2.21.6]

The consolidated raw transactional logs shall, in real-time or near real-time, update a transactional log database. The transactional log database shall order all SIP transactions by the initial time-stamp (PTZ) of the first INVITE, and group related transactions (such as identical SIP Call-ID headers) under this initial entry. ALI transactions shall be similar in that the order will be by initial time-stamp of the initial bid for the call (ANI/pANI) and grouped by response and any subsequent re-bids.

Transactional logs will be updated and grouped as specified.

7.2.21.7. Database Search – [RFP 6.2.21.7]

In the transactional log database, the most commonly utilized SIP headers (To:, from:, Contact:, etc.) and the request URI shall be parsed into dedicated fields into the transactional log database for easy searching and interpretation.

Transactional logs will be parsed in the database as specified.

7.2.21.8. Database Tools – [RFP 6.2.21.8]

BIDDERS shall provide a consolidated log searching, reporting, and counting tool(s), supporting at least the following functions:

- *Retrieval of any group of transactions, including related ALI Database transactions, related to a single call identified by time (PTZ), calling number, source, ultimate destination, or SIP Call-ID header.*
- *Retrieval of a set of calls based on source, ultimate destination, calling number, and conditioned by some specified interval of time*



- Generate call volume reports (counts) based on source destination, call handling (e.g., success, failure (reason), transferred, etc.) over an interval of time.

The tool set shall be web-accessible and shall support the creation of new reports based on user specified selection and output criteria.

Our [12a] allows for grouping of calls with their ALI transactions, retrieval of calls by time stamp or destination, and reporting on calls with their success criteria. Every transaction is recorded in our system, and customized reports can be developed by identifying the correct fields and generating custom queries. The database tools will be web accessible.

7.2.21.9. Database Access – [RFP 6.2.21.9]

BIDDERS shall provide a secure (e.g., two-factor authentication) web portal or other means allowing MIL (administrators) read-only access to the transactional log database and log inspection tools. These users shall be able to generate and print their own reports from the data in the transactional log database.

TCS' partner, [12a], will provide a secure portal to obtain the raw log information that can be ingested and saved. The [12a] ad hoc tool can be used to create reports against the transactional logs, and reports also can be shared among other [12a] portal users within the Washington instance (if users elect to share).

7.2.21.10. Operational Log Events – [RFP 6.2.21.10]

At a minimum, all elements, processes or services shall process and date/time-stamp operational log entries into the dedicated local raw operational log files and into an operating system logging facility (such as Linux "syslog" or Windows application logs) for the following date/time-stamped events:

- Every time the process is started, and any relevant details of how it was started (e.g., command line, monitor program, startup parameters, etc.).
- Any major change in the process state, such as process going from on-line to standby, shutting down, etc. If possible, a change of process state should be accompanied by a reason, e.g., "operator commanded shutdown", or "memory overflow".
- Significant non-routine events, including "TCP session failed/established by <IP address>", "connection to <process name>" lost, "error encountered in in config file line xx", "Bad location data with call <call-id>".

If the process supports operator logins, the operational log shall show every login attempt, user and time, successful or unsuccessful, the operator commands issued, and logout time.

All requested items are currently logged in our system using syslog servers and application logs. User transactions are also logged. The local raw files are collected into our [12a], where further processing is possible as needed.

7.2.21.11. Operational Log Tools – [RFP 6.2.21.11]

BIDDERS shall provide a search and report generating tool, with secure access (e.g., two factor authentication), that can promptly and safely search the consolidated operational logs for all entries or some interval pertaining to a specific element, process, or services, or a specific instance of a process or service. The tool shall also support retrieval of all operational log entries over a specified interval of time, and conditioned for a specific type of entry, keyword, or key phrase. This tool may operate (via read-only access) on the consolidated raw operational log file, or upon some operational log database derived from the operational log files, at the BIDDER's discretion.

For operational log data, users will access our [12a]. Only authorized users will have access; they will be allowed to search the database for transactions using a variety of methods.

If transaction data is to be analyzed, [12a] provides the secure [12a] portal for all analytics and query of data collected within the ESInet. A combination of standard "canned" reports and ad hoc interfaces for querying the data is provided, as well as access to data analysts



as part of the service for requesting large datasets and analysis. The analysts assist when there is a need for deeper analysis that requires an expert in statistics and analysis.

7.2.22. Monitoring Dashboard – [RFP 6.2.22]

Experienced BIDDERS will be aware that monitoring dashboards are a quick and effective way to review performance of a network at a glance and often incorporate them into their NOCs. In a similar vein, MIL highly desires this capability within our EOC and to allow access to same by the individual 911 Authorities as well. As such, the following requirements identify the minimum features that MIL desires, but BIDDERS are encouraged to provide a capability that goes beyond these requirements.

7.2.22.1. Network Monitoring Dashboard – [RFP 6.2.22.1]

BIDDER shall provide a web-based dashboard that displays the operational status of the facilities (e.g., MPLS hops, T1's, etc.) and elements (i.e., LNG, BCF, ESRP, ECRF, LVF, GIS, NLIS, and Gateways) that comprise the ESInet within one-year of system turn-up (i.e., all PSAPs migrated).

7.2.22.2. Graphical Display – [RFP 6.2.22.2]

Status information shall be displayed in a graphical manner in which each element is depicted by icon that is unique to the element and shows the IP interconnections between each element. Individual routers/switches do not have to be depicted, but any failure and/or impairment of the IP interconnection due to a failure or performance impacting condition of a router/switch shall be reflected in the status of the interconnection displayed. Full monitoring system functionality must be available with one year of system turn-up.

7.2.22.3. Near-Real Time Display – [RFP 6.2.22.3]

Status information should be updated every sixty (60) seconds.

7.2.22.4. Operational States – [RFP 6.2.22.4]

Facilities and elements shall display their operational status as indicated below. The use of colors is highly encouraged, but left to the BIDDER to determine the most effective methodology to inform the user.

- Fully Operational (green)
- Operationally Impaired e.g., congestion (orange)
- Failed (red)

7.2.22.5. Display Drill-Down – [RFP 6.2.22.5]

If a displayed element and/or facility is an aggregate object (e.g., an implementation in which the PRF is a sub-component of the ESRP), it shall be possible to click (i.e., right or left computer mouse click) on the displayed object to expand the view to show all elements comprising the originally displayed object.

7.2.22.6. Dashboard Access – [RFP 6.2.22.6]

A user name and password shall be required to access and display the dashboard. Provision should be made for up to 75 named users and 55 simultaneous users.

7.2.22.7. Browser – [RFP 6.2.22.7]

While support for all popular web-browsers is desirable, Internet Explorer 10 is MIL's preferred web-browser.

7.3. Support for Multi-Node PSAPs [RFP 6.3]

Multi-Node configurations consist of two primary, or "Host", PSAPs interconnected to form a singular logical PSAP which is in turn interconnected to distant or remote PSAPs.



7.3.1. Multi-Node: Host-to-Host Connectivity – [RFP 6.3.1]

At time of this RFP, only TCOMM and CERSA are operating in a Multi-Node configuration, but as yet have no operational Remotes. However, several PSAPs are considering becoming Remotes and others may be considering their own Multi-Node deployments.

Accordingly the BIDDER should be aware that providing connectivity between Hosts and/or between Hosts and remotes may be requested from the BIDDER at a future date. MIL understands that the BIDDER cannot provide detailed pricing information until the locations are known, but we are requesting that the BIDDER provide the cost elements for access methodologies they plan to offer, including any distance sensitive components.

The BIDDER may also wish to consider the following requirements and their impact on any cost elements.

We understand the requirements for operating multi-node PSAPs. Our network engineering team will be responsible for provisioning and maintaining the connections, and they will do so once detailed information is obtained. Typically, depending on the difficulties in reaching a multi-node site(s), connectivity will be provided either by private circuits (e.g., private fiber networks) or commercial carrier. Either option is acceptable, and we will support the network as part of the 9-1-1 infrastructure.

7.3.1.1. Connectivity Monitoring – [RFP 6.3.1.1]

All connectivity between Hosts and/or Host-Remotes must be monitored on a 365X24X7 basis as identified for ESInet connectivity elsewhere within this RFP. Ideally, the monitoring should be performed by the same NOC as is monitoring the ESInet. However, if this is not feasible (i.e., different providers) the BIDDER is expected to provide process and procedures to insure all NOCs have a high-level view (albeit perhaps not real-time) of the operational status of all facilities carrying 9-1-1 traffic.

We fully expect to monitor and manage the connection between hosts and remotes using the same processes and monitoring network in use for the rest of the ESInet. [12] NOC would monitor all connections in the solution.

7.3.1.2. Connectivity Service Level Agreement (SLA) – [RFP 6.3.1.2]

All facilities used to provision primary connectivity between Hosts and/or Host-Remotes should meet the Washington State SLA identified in Section 7.8

We would intend all facilities to meet the SLAs as described. In the instance that a specific request to use certain circuits (e.g., private fiber) that do not meet the SLA requirements is made, we will note the deficiency for approval by Washington prior to implementing the circuit(s).

7.4. Facilitating Carrier Transition – [RFP 6.4]

The BIDDER shall be responsible for the migration of existing 9-1-1 services to the ESInet and to NG9-1-1 services at all interfaces between the BIDDER and other emergency call originating network operators in order to accomplish 9-1-1 call delivery which meets the quality and reliability requirements of this RFP. This includes stating the terms, conditions, procedures, or processes for interconnection and exchange of information between other carrier's networks and systems and the BIDDER's networks and systems. Unless the parties otherwise agree, such terms, conditions, procedures or processes shall follow any applicable Washington State laws, telephone industry practices, NENA standards and recommended practices, or applicable US telecommunication law. The terms, conditions, procedures or processes shall not impose onerous requirements on other network operators, and shall be stated in the proposed solution. Examples of such interfaces would be the means to perform the timely exchange of information such as legacy ALI database updates, exchange of monitoring/trouble ticket status, trunk connections to the LNG, and IP connections to Border Control Function(s). This list of examples is not exhaustive. The BIDDER is expected to work closely with other network operators and to cooperate fully with them in order to accomplish successful transition to the i3-based ESInet.

We are practiced in deploying statewide ESInets and fully expect to work very closely with other network operators to implement this transition. We will follow all applicable laws, practices,



and guidance that would be expected of such a transition. In order to best facilitate the change to the i3 ESInet, we will work with the providers (under a letter of authority from the state) to implement the changes needed to successfully bring the traffic onto and through the ESInet.

The professionals who staff the TCS PMO have extensive training and experience with managing complex, multi-tiered projects. They are fluent in managing ESInet, IP-based call handling, ALI DBMS, and GIS implementations. The project managers speak the language of 9-1-1 and can actively help navigate project complexities. These professionals all come from the 9-1-1 industry and/or have real-world experience with GIS/IP technologies. Project management ensures that these solutions meet our customers' needs, even beyond project implementation and cutover.

This team provides all the guidance necessary for our customers to successfully transition to the TCS NG9-1-1 solution.

Because of the critical nature of a 9-1-1 system, projects are implemented in a phased approach to isolate changes and minimize negative impact. Each project requires a predictability model and a worst-case scenario model to ensure that project participants are ready to deal with any situation that may arise during the implementation process. Once this model is designed, project risk is measured and plans are adjusted accordingly. Our project managers closely monitor every project, seeking out early signs of risk and ensuring that action plans are working properly. Project managers also establish a project steering committee for every project.

The assigned project manager will provide documentation related to the system that covers the following elements:

- A communications plan, with contact information for all involved resources
- A PROJECT PLAN, including detailed tasks, allocated resources, dependencies, and milestones
- A product questionnaire to identify specific, desired systems settings and configurations
- A system ATP
- Standard technical and maintenance information
- As-built diagrams and drawings of the system's layout and design.

The above-listed bullets are intended to aid stakeholders in the deployment of the system. Any conditions contained in these documents will be in accordance with normal industry practices and will not impose onerous requirements on other network operators.

The overarching plan involves a number of stages that are intended to bring about an orderly systems launch.

Planning – The first stage is planning. This includes a review of existing documentation as well as site surveys for each location. We will work with Washington to perform and document system data collection activities, with special attention given to such unique site conditions as space constraints, wiring requirements, telco demarcs, etc.



Ordering – Next is the ordering stage, where hardware, peripherals, and software are identified and purchased for eventual distribution to their respective locations. Finally, each collection point is prepped to accept these shipments.

Staging – In staging, everything is received and documented at each collection point. Raw material is inventoried, software is loaded onto its respective hardware and properly configured, and all items are double-checked against stocking manifests that have been drawn up for all the locations. The final step in this process involves delivery to each respective site.

Installation – The installation stage, which is minimal as it pertains to PSAPs, includes such elements as site preparation, running cable, populating the PSAP-provided racks with the proper hardware, and checking for proper power levels and network connectivity. All personnel charged with performing the installation of this proposed solution have considerable field experience in IT and/or telecommunications. We have dedicated facility managers who will install the systems in the CLCs [12a]

Transition – The transition stage involves two separate processes. Training, if deemed necessary, will be held at the designated customer site for end users and administrators. Meanwhile, core network testing will be under way. Offline test calls for the new 9-1-1 system to be conducted for each location, including incoming wireline, wireless, and VoIP transmissions.

Cutover – The cutover stage will involve a phased approach that starts at the CLCs and progresses to each PSAP.

Our backout plan isolates all system traffic from the live environment. [12a]

On the following pages is the detailed transition plan.



TeleCommunication Systems, Inc.
Transition Plan

Washington State ESInet

TeleCommunication Systems Inc. (TCS)
2401 Elliott Avenue
Seattle WA 98121
Phone 206.792.2000
Fax 206.792.2001
www.telecomsys.com



**TCS – Hosted Service Platform
Small-Market Transition Plan**

January 2016

TCS Confidential: [Proprietary Level 2](#)



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

TCS Point of Contact

Danny McGinnis

Phone: 206.792.2672

Email: dmcginnis@telecomsys.com

Table of Contents

- 1. Purpose of This Document and Intended Audience 3
- 2. NG9-1-1 Customer Kick-Off Meeting 3
- 3. Program Management 4
- 4. Data Gathering and PSAP Readiness 4
- 5. [12a] PSAP On-boarding and Transition Process 5
- 6. [12a] Carrier On-boarding and Migration Process 7
- 7. Transition Process Diagrams 7
- 8. Additional Information 9
- 9. [12a] Carrier and PSAP Transition to TCS ALI DBMS (TCS ALI)..... 10
- 10. [12a] Ongoing NG9-1-1 Lifecycle Program Management..... 12



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

1. Purpose of This Document and Intended Audience

This document is an overview of the Next Generation 9-1-1 (NG9-1-1) transition plan used by TeleCommunication Systems, Inc. (TCS) when transitioning public safety answering points (PSAPs) and carriers to the TCS Hosted NG9-1-1 Service Platform. The audience for this document is:

- Personnel from Washington State's 9-1-1 program
- Other vendors associated with Washington State's NG9-1-1 transition

The information in this document will help you gain a solid understanding of the steps TCS takes to assist new NG9-1-1 customers through a successful transition from another vendor's legacy or NG9-1-1 selective routing (SR) services and Automatic Location Identification (ALI) database management services (DBMS) to the TCS Hosted NG9-1-1 Service Platform.

2. NG9-1-1 Customer Kick-Off Meeting

TCS will hold a customer kick-off meeting shortly after signing the contract and/or when the statement of work (SOW) is completed. The customer kick-off meeting is the first step in the transition process. During the meeting, TCS staff will meet with staff from the State of Washington and key stakeholders to review the transition process, gather data, and ensure that all parties agree on components within the SOW. In addition, site visits to the Washington State PSAPs will be conducted.

The following documents will be provided and reviewed to guide discussions:

- SOW
- NG9-1-1 call and data flow diagram(s)
- View of transition from existing 9-1-1 solution to TCS NG9-1-1 solution
 - [12a] On-boarding PSAPs onto the TCS NG9-1-1 selective routing network (Emergency Services IP Network [ESInet])
 - [12a] On-boarding carriers onto the TCS NG9-1-1 selective routing network (ESInet)
 - [12a] ALI database transition
 - [12a] and beyond: TCS ongoing NG9-1-1 Lifecycle Program management

The different transition phases [12a]
 This is based on our experience [12a]
 and [12a]
Note NG9-1-1 transition work we have done with our channel partners. We will start next phases well before the previous phase is complete. Each phase is complete once carrier testing and/or PSAP testing is verified. Our transition plan phases are run in parallel until all phases are complete.

- Communication Plan
- Network-level alternative call routing (last routing option [LRO] plus potential regional large call centers handling certain alternative routing scenarios)
- TCS letter of agency (LOA)



- Change Management Request form

3. Program Management

During the transition stage of the NG9-1-1 program lifecycle, it is expected that the State of Washington and TCS Client Services contact [12a] will be in regular contact.

Weekly conference calls with TCS will help the state, TCS' client service manager, and other key stakeholders review progress, plan for upcoming project deliverables, and address issues that might affect the timeline.

When each phase of the transition is complete and the state's carrier and PSAP operations have been migrated to the TCS Hosted NG9-1-1 Services Platform, TCS will continue to hold regularly scheduled calls. TCS' client service manager will set up the calls at agreed-upon intervals and will manage day-to-day program needs (other than incident resolution).

Note Contact the TCS Network Operations Center (NOC) should incidents arise at a PSAP relating to NG9-1-1 service.

Change management will be handled according to the change management process, which TCS will provide during the transition.

4. Data Gathering and PSAP Readiness

Before beginning transition, the following data is gathered. This data is necessary to ensure the successful transition of carriers and PSAPs to TCS' NG9-1-1 solution.

- PSAP site survey workbook (some data may already be provided by the state prior to PSAP site visit)
 - General administrative information
 - Type of operation (primary PSAP, secondary PSAP, or regional group of PSAPs with shared controller)
 - Number of call-taker positions at each PSAP
 - PSAP equipment inventory (controller, rack space, power supply, and other information deemed necessary during the PSAP site tour)
 - Whether there is adequate rack space and power available for the PSAP's NG9-1-1 on-boarding process
 - TCS also would like to take pictures of the rack space and customer premise equipment (CPE) ports to help us with any troubleshooting issues as we transition and support PSAPs day to day
- Alternative routing plans for each PSAP
- Speed-dial (also known as star code, one-button transfer, or pound key) list for each PSAP
- Wireless, Voice over Internet Protocol (VoIP), and wireline call volume by month per PSAP



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

- Connection type to TCS' NG9-1-1 solution will vary based on the PSAP Automatic Number Identification (ANI)/ALI controller capabilities.
 - For controllers that are *not* Session Initiation Protocol (SIP)/I3 capable, a connection will be made via Centralized Automatic Message Accounting (CAMA) trunks to a new 66 block installed by TCS. The PSAP's CPE vendor will connect into this demarcation.
 - For controllers that are SIP/I3 capable, connections will be made via an Ethernet connection. Specifications for this connection will be sent within 30 days of the state providing TCS with the controller make and model and the software version of the CPE. TCS would also like the contact information for the state's CPE vendor.
- A copy of the ALI format (aka ALI spill) for 9-1-1 calls. *Note:* The state should be able to obtain the standard format supported by its incumbent vendor(s) as a starting point, but TCS will need to confirm if the PSAP requested any changes to the standard.

Other miscellaneous information may be required based on the final high-level architectural design and PSAP data. Please note, until this information is obtained, TCS cannot officially start the PSAP or carrier transition process to the TCS NG9-1-1 solution. Also note that TCS will need to re-verify some of this data no later than 15 business days prior to the PSAP's test date.

5. [12a] PSAP On-boarding and Transition Process

TCS gets the PSAPs ready for the transition in parallel with the carrier transition process. Process steps include:

1. Ordering PSAP site equipment

When the PSAP site survey information has been gathered and TCS verifies the type of controller at each PSAP, TCS orders the necessary equipment. It may be the PSAP's responsibility to ensure that the required rack space is available and that power needs are met prior to TCS installing the PSAP site equipment.

Note

If, during the PSAP site visit, TCS identifies any environmental constraints to hosting the NG9-1-1 equipment, the PSAP and its technical representatives will be notified prior to TCS ordering the equipment. It is either the state's or the PSAP's responsibility to resolve these constraints prior to TCS installing the equipment. Issues may involve rack-space expansion, power and heating/cooling requirements, or demarcation extensions.

TCS engineers design and build the circuits necessary to connect the PSAP to the TCS NG9-1-1 Service Platform. TCS configures the PSAP's site equipment based on the architecture design for the customer.

The equipment will be shipped to the PSAP, and TCS will let PSAP staff and/or vendors know when to expect shipment.

TCS wants the state to understand that TCS is well versed in handling the transition of PSAPs connected into a shared regional controller (CPE) design.

SIP Interface Specification

TCS provides this specification to the state's PSAPs to share with their CPE vendor after TCS provides its initial high-level architectural design document

January 2016

Copyright 2012 TeleCommunication Systems Inc.
 TCS Confidential: [Proprietary Level 2](#)

5
 TCSP-287



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

to the state. TCS has a standard specification, specification; however, TCS wants to be certain it understands all architectural design considerations prior to sending out any specifications.

2. Installing PSAP site equipment

A TCS engineer will visit the PSAP to install the NG9-1-1 equipment and circuits. The engineer will need access to the rack space where the equipment will be installed. The TCS client service manager will contact the state to coordinate installation in advance of the installation. A target date for this installation will be included in a project plan that will be provided after the kick-off meeting.

In the case of regional PSAPs sharing a single controller, TCS typically hosts a meeting so all PSAP personnel connected into the shared controller have an opportunity to weigh in on the transition and their needs.

3. Interconnection to incumbent's ESInet

When TCS receives the state's LOA and the necessary PSAP data, TCS will contact the incumbent ESInet service provider to set up a series of technical discussions regarding connectivity to the incumbent to enable transfers and call delivery during the cutover transition period.

TCS will initiate circuit orders into the incumbent network and complete testing of commercial off-the-shelf (COTS) equipment once circuits are installed. We provide an interface control document (ICD) to the incumbent service provider and start validation review with the incumbent to ensure the edge applications will interoperate as required.

TCS will then create an interoperability test plan for review with the incumbent service provider. TCS and the incumbent service provider will perform and document the results of the interoperability testing.

4. Pre-audit testing

TCS application engineers conduct a pre-audit test to ensure that TCS has provisioned necessary PSAP data correctly in the system. TCS will validate the transport into the PSAP and conduct other functional audit tests that ensure PSAP testing is successful in the next step.

5. PSAP testing

TCS has provided a draft of its standard NG9-1-1 PSAP Acceptance Test Plan (ATP). TCS developed this plan based on its experience transitioning more than 200 PSAPs to a TCS NG9-1-1 platform. We will work with the state of Washington to fine-tune our existing test plan if needed.

It is the PSAP's responsibility to take the following steps in support of testing in order to successfully complete the PSAP's migration to NG9-1-1:

- Notify their CPE vendors prior to testing so:
 - The controller vendor can configure the new ports prior to the test start time. On the day of testing, the controller vendor should be available to support testing.
 - The recording (data and voice) vendor can validate that changes to the PSAP's controller SAP will not affect recording. If they might, TCS recommends that the vendor be available to support testing.
- Be sure there is a person on-site to make test calls.
- Be sure there is a 9-1-1 dispatcher available to accept test calls.

January 2016

TCS Confidential: [Proprietary Level 2](#)

6
TCS-287



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

TCS will coordinate and host a conference call for all participants involved in the testing. After all parties agree that testing was successful, TCS will send a go-live notification via email indicating that the PSAP is ready to transition to the NG9-1-1 Hosted Service Platform.

Note: TCS' go-live process can include automatically cutting the PSAP over if all parties agree to that based on successful testing. TCS test plans include a rollback process in the rare case a PSAP test is unsuccessful.

6. [12a] Carrier On-boarding and Migration Process

Routing Calls Directly to the TCS NG9-1-1 Hosted Service Platform

Carriers will connect directly to the TCS points of ingress, and TCS will work with the state and its carriers to manage the migration. Based on TCS' experience working with wireless and other carriers, the carriers require six months' notice to transition to another SR and/or ALI service provider. TCS will need to obtain the following information to start the process of on-boarding carriers:

- Name and contact information for all carriers operating in the state of Washington who will connect into the NG9-1-1 network
- Letter of authorization from the state (TCS can provide a draft)

Prior to starting work with the incumbent service providers, it is critical that all PSAP-related data be procured. TCS will start working with the incumbent SR service provider as soon as possible thereafter.

Once the state has provided TCS with the LOA and contact information for all carriers operating in the region, TCS will give the carriers a Method of Procedure (MOP). The MOP contains the following information:

- How to get started
- Provisioning of facilities
- [12a] or SIP ingress
- TCS carrier data requirements
- Testing and turn-up requirements
- Network monitoring/trouble and outage reporting information

Once the carrier has been successfully tested and transitioned to the TCS NG9-1-1 platform, the carrier will want to remove its trunks from the legacy or other next generation incumbent service provider's router. TCS recommends that the appropriate state 9-1-1 authority convey the amount of time it expects the carriers to maintain their trunks (aka the soak period) prior to removal.

7. Transition Process Diagrams

A two-page diagram summarizing TCS' transition plan follows.



Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

[12a]





Washington State Military Department
Next Generation 9-1-1 Emergency Services Internet Protocol Network
Statement of Work | June 24, 2016

[12a]





TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

Call Transfers to PSAPs Outside the TCS NG9-1-1 Network

We understand some of the state's PSAPs will transfers calls to PSAPs outside the TCS NG9-1-1 network. As a result, we may need to order trunks into other legacy or next generation SRs that serve those out-of-state PSAPs. We have noted the need to connect into the Washington PSAP connected via the Navy's ESInet. We have already completed interoperability testing in Texas with the Navy's current ESInet service provider, and we will plan additional testing from TCS' Washington ESInet. Please note that this is one of the longest lead time tasks when transitioning a state's PSAPs to an NG9-1-1 network. We must order trunks into any non-TCS SRs and other networks as early as possible, based on our final transition plan.

In order to start the process of ordering these trunks, TCS will need the PSAPs' speed dial and alternative routing information, along with the projected number of calls transferred via the PRI lines.

GIS Readiness

As addressed in TCS' RFP response, TCS will work with [12a] so the Geographic Information System (GIS) data meets the state's accuracy requirements. Once those requirements are met, we will plan to transition use of the state's GIS data in the appropriate call-routing scenarios.

In the meantime, TCS is able to transition using the existing legacy Emergency Service Number (ESN) routing method along with typical default and alternative routing scenarios available with TCS' ESInet service.

9. Phase 2: Carrier and PSAP Transition to TCS ALI DBMS (TCS ALI)

TCS will kick off the transition plan to get the carriers and PSAPs ready for the TCS ALI DBMS transition within 90 days of starting Phases 1a and 1b. Process steps include:

1. Gathering existing ALI and MSAG records

TCS will need the State of Washington to provide the current statewide ALI and MSAG data from its existing 9-1-1 service providers.

The TCS ALI Quality and Process Service (AQPS) team takes the existing data and analyzes it to determine correct sizing of the state's ALI DBMS as well as the number of carriers who will load data into the ALI. This may differ from the carriers who on-boarded onto the ESInet, given many carriers load data with more than one NENA ID. We also evaluate who will need user accounts to access the ALI DBMS processes. Finally, TCS' AQPS team analyzes any MSAG or ALI records to see if the incumbent service providers have loaded records that do not meet NENA standards. We will build scripting into our bulk-loading processes to handle this type of anomaly.

2. Finalizing transition plan for this phase of the migration onto TCS' solution

TCS will determine the best plan to transition PSAPs off the incumbent's ALI DBMS and onto the TCS ALI DBMS. Factors will include if or when the PSAPs' Phase 1a ESInet migration has occurred, special requirements such as call transfers to out-of-state or off-network PSAPs, and whether the PSAP is operating and will continue to operate its own stand-alone ALI.

3. Notifying carriers of the ALI DBMS transition plan

The transition plan provides:

- The state's LOA

January 2016

TCS Confidential: [Proprietary Level 2](#)10
TCS-287



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

- Instructions for carriers and transition details (e.g., dates we will provide training on ALI DBMS processes, when carriers will be targeting dual provisioning, etc.)
 - Targeted PSAP cut dates
 - Carrier-side ALI User Guide
4. Gathering additional PSAP data to support ALI transition
- TCS prefers the current service provider(s), CenturyLink and/or its vendor Intrado, provide the key ALI data that follows, but we may need to gather the data directly from the PSAPs.
- English language translations (police, law, fire, EMS)
 - ALI format (aka PSAP spill), if not stateside format

At minimum we verify this data 30 days before a PSAP cut to TCS' ALI DBMS.

5. Building the ALI DBMS
- During this step TCS uses the PSAP and carrier data gathered earlier in the transition process to build the DBMS tables.
6. Completing carrier and PSAP ALI DBMS training and verification testing
- TCS typically conducts a series of ALI DBMS training webinars based on the ALI transition plan. We can perform on-site regional training per our contract and/or SOW requirements. Our training is based on the type of end user being trained. Carriers and PSAPs get their own training sessions, and User Guides are based on the workflows each trainee will utilize.

Once we have completed training and set up user accounts on the ALI DBMS, we ask users to do a simple verification test to ensure they can access the ALI DBMS processes they will be using.

Toward the end of this stage TCS does at least two bulk data loads and validation testing of the current MSAG and ALI telephone number records (TNRs). Based on the number of TNRs that validate during the bulk load process, we determine if we've met the state's validation requirement. Our experience shows most states want at least 95 percent of the existing TNRs to load without errors.

We work with the carriers and/or PSAPs to resolve validation errors. It should be noted that a small percentage of the TNRs will not validate during this process, but this should not stop the state's ALI transition. The TCS AQPS team will consistently work these types of validation errors through TCS' automated, web-based ALI discrepancy and MSAG change management processes.

7. Performing PSAP testing – ALI format data

As with [12a] testing, TCS provides a standard test plan, except in this case it's based on validating the ALI format data spilled at the time of the test call. The test will:

- Validate the ALI spill meets the PSAP format determined earlier in the process
- Verify call data for various classes of services

TCS will work with the state of Washington to solidify its ATP requirements.

January 2016

Copyright 2012 TeleCommunication Systems Inc.
 TCS Confidential: [Proprietary Level 2](#)

11
 TCSP-287



TeleCommunication Systems, Inc.

Washington State ESInet Transition Plan

It is the PSAP's responsibility to take the following steps in support of testing in order to successfully complete the PSAP's migration to the ALI DBMS:

- Notify their CPE vendors prior to testing so:
 - The controller vendor can configure any new PSAP ALI format changes. On the day of testing, the controller vendor should be available to support testing.
 - The recording (data and voice) vendor: Validate that changes to the PSAP's controller SAP will not affect recording. If they might, TCS recommends that the vendor be available to support testing.
- Be sure there is a person on-site to make test calls.
- Be sure there is a 9-1-1 dispatcher available to accept test calls.

TCS will coordinate and host a conference call for all participants involved in the testing. After all parties agree that testing was successful, TCS will send a go-live notification via email indicating that the PSAP is ready to transition to the NG9-1-1 Hosted Service Platform.

Note: TCS' go-live process can include automatically cutting the PSAP over if all parties agree to that based on successful testing. TCS test plans include a rollback process in the rare case a PSAP test is unsuccessful.

10. [12a] Ongoing NG9-1-1 Lifecycle Program Management

After a PSAP is tested and transitioned and is live on the TCS NG9-1-1 ESInet and/or the ALI DBMS service and platform, the PSAP is in the management and maintenance phase of the NG9-1-1 program lifecycle. The PSAP is supported by TCS NOC incident management processes and TCS' operational program lifecycle change management processes, backed by the NG9-1-1 program management team.

TCS will provide its PSAP standard operating procedures (SOPs) as well as training for the state and PSAPs on how to contact TCS for 9-1-1 troubles or change management.

TCS looks forward to supporting you, our new NG9-1-1 customer, throughout your NG9-1-1 program lifecycle.



7.4.1. Conversion of Legacy (CAMA) PSAPs – [RFP 6.4.1]

As only some of the PSAPs are likely to be converted from CAMA to the i3 architecture by the time of implementation of a contract, BIDDER shall be required to provide installation oversight of the network interface as each remaining legacy PSAP converts to the i3 architecture.

Installation and oversight activities shall include:

- *Comprehensive Site Survey (ESInet interface hardware/software)*
- *Installation Design Specification*
- *Ensure compliance to deployment specifications*
- *Stage any required Installation Related Material*
- *Installation Project Management*
 - o *Coordination with i3 CPE Project Manager*
 - o *Coordination with and approval from MIL*
- *Produce progress reports to MIL and 911 Authorities*
- *Perform Customer Walk through and Acceptance*
 - o *BIDDER, in conjunction with MIL, will develop and provide Acceptance Test Plan (for connection to the ESInet)*

Provide "As-Built" documentation to MIL, the County 911 Authority and the PSAP; two (2) copies each.

As previously described, we are well-versed in the deployment of ESInet solutions that have either legacy or IP-capable CPE at the PSAPs. In particular to legacy PSAPs, our installation and cutover will include LPGs to interface with the ESInet and the CAMA trunks.

Our detailed process includes all preparation work needed with the PSAP and CPE vendor, including site survey, network equipment installation and configuration, initial testing, cutover, and all communications. We will follow our ATP in all instances, and our configuration and change management process will ensure that each cutover has the highest possible probability of success. Issues that cannot be corrected during the cutover will result in a structured roll-back of the cut. After the successful cutover, we will provide the necessary as-built documentation.

7.4.2. Direct IP-Connected PSAPs – [RFP 6.4.2]

Currently there are 18 PSAPs that connect their CPE directly (i.e., no CAMA conversion) to the ESInet via the RFAI protocol, see Attachment I, supported by the incumbent ESInet provider. It is estimated that as many as 30+ PSAPs will be operating in this mode by the time the i3-based ESInet is ready to go in-service. To facilitate interworking with these PSAPs MIL requires that:

- 1) *The BIDDER will simultaneously support both the RFAI interface AND the new i-3 based interface, OR;*
- 2) *Provide a detailed plan of how these PSAPs can be transitioned to the i3-based ESInet at time of cut-over WITHOUT ANY INTERUPPTION IN SERVICE. Experienced BIDDERS will understand that this plan need also address coordination with the PSAP and PSAP CPE vendor in order to reverse any software upgrades/changes that were made to interface their CPE via the RFAI interface.*

We already support both the i3 and the RFAI interfaces in other large-scale deployments of our ESInet. We are familiar with the coordination required to migrate RFAI-capable PSAPs onto the network, and we have written a module into our code to enable communication to RFAI CPE. Given our ESInet RFAI interface module, the conversion process for RFAI-capable CPE is no different than any other PSAP conversion.