COMTECH TELECOMMUNICATIONS CORP.

www.comtechtel.com

68 South Service Road, Suite 230, Melville, New York 11747
Tel: 631.962.7000 • Fax: 631.962.7001

March 4, 2016

Leah Missildine
Interim Executive Director
Alabama 9-1-1 Board
1 Commerce Street
Suite 610
Montgomery, AL 36104
334.440.7911
leah@al911board.com

Subject: AL-NG911-RFP-16-001 Alabama Next Generation 9-1-1 Systems and Services

Dear Ms. Missildine,

TeleCommunication Systems, Inc. (TCS), a wholly-owned subsidiary of Comtech Telecommunications Corp., is pleased to respond to the state of Alabama's Request for Proposal (RFP) for Next Generation 9-1-1 (NG9-1-1) systems and services.

TCS acknowledges, understands, and agrees with the general information presented in Section 1 of the RFP general instructions. TCS is capable of meeting the requirements of Section 2.3 of the RFP general instructions. TCS is willing to provide the requested products and/or services subject to the terms and conditions set forth in the RFP, including the mandatory contract clauses. Included in the business volume is the annotated sample contract with changes we deem appropriate to negotiate.

TCS acknowledges receipt of RFP Addenda 1, 2, and 3.

Our point of contact for this effort is:

David Gleason
Regional Account Manager
TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401
Mobile: 802.473.2005
Fax: 410.280.4903
david.gleason@comtechtel.com

TCS appreciates this opportunity to provide its response and looks forward to working with you.

Sincerely,

Dr. Stanton D. Sloane
President and Chairman of the Board of Directors
TeleCommunication Systems, Inc.

Alabama Next Generation 9-1-1 Systems and Services

AL-NG911-RFP-16-001

Business Proposal

March 4, 2016

Submitted to:

Leah Missildine
Interim Executive Director
Alabama 9-1-1 Board
Reference: AL-NG911-RFP-16-001
1 Commerce Street
Suite 610
Montgomery, AL 36104
334.440.7911
leah@al911board.com

Prepared by:

TCS TeleCommunication Systems
Enabling Convergent Technologies®

David Gleason
Regional Account Manager
TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401
802.473.2005
david.gleason@comtechtel.com
www.telecomsys.com

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®, 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™, 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 439 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.

Table of Contents

1. Transmittal Letter 1
2. Executive Summary 2
2.1. Meeting Alabama's Objectives 2
2.2. Solution Benefits 2
2.3. Solution Components 2
2.3.1. Base Solution 2
2.3.2. Options 4
2.3.3. Cost Savings 4
2.4. TCS CLEC Subsidiary 4
2.5. Valid Pricing Period 5
3. Annotated Sample Contract [RFP Attachment A] 6
4. Business Proposal Spreadsheet [RFP Attachment B] 23
4.1. Respondent's Company Structure [RFP 2.3.2] 23
4.1.1. TCS Company Leadership 23
4.1.2. Safety and Security Technologies Leadership 24
4.1.3. Certificate of Authority 24
4.2. Authorizing Document [RFP 2.3.8] 26
4.3. Subcontractors [RFP 2.3.9] 27
4.3.1. Direct Technology 27
4.3.2. GeoComm 28
4.4. General Information [RFP 2.3.10] 31

List of Exhibits

Exhibit 1. Safety and Security Technologies Organizational Chart 24
Exhibit 2. Certificate of Authority 25
Exhibit 3. Authorizing Document 26
Exhibit 4. Table of Contents from TCS' Established Disaster Recovery Plan 32

Glossary

Term	Definition
ACL	Access List
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
AL9-1-1	Alabama 9-1-1 Board
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AP	Access Point
AQPS	ALI Quality Process Services
ASA	Alabama Supercomputer Authority
ATIS	Alliance for Telecommunications Industry Solutions
B2BUA	Back-to-Back User Agent
BCF	Border Control Function
BGP	Border Gateway Protocol
CAD	Computer-Aided Dispatch
CAMA	Centralized Automatic Message Accounting
CBWFQ	Class Based Weighted Fair Queuing
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
CoS	Class of Service
COTS	Commercial Off-the-Shelf
CPE	Customer Premise Equipment

Term	Definition
CSA	Canadian Standards Association
CSP	Communications Service Provider
CSRIC	Communications Security, Reliability and Interoperability Council
CVSS	Common Vulnerability Scoring System
DACS	Digital Access and Cross-Connect System
DBMS	Database Management System
DNS	Domain Name Server
DoD	Department of Defense
DoS	Denial of Service
DSCP	Differentiated Services Code Point
E9-1-1	Enhanced 9-1-1
ECaTS	Emergency Call Tracking System
ECD	Emergency Communications District
ECRF	Emergency Call Routing Function
EIA	Electronic Industries Alliance
E-MF	Enhanced Multifrequency
EMI	Electromagnetic Interference
ESA	Emergency Service Agency
ESGW	Emergency Services Gateway
ESIND	Emergency Services IP Network Design
ESInet	Emergency Services IP Network
ESP	Enterprise Security and Protection
ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Proxy
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
GIS	Geographic Information System
GMLC	Gateway Mobile Location Center

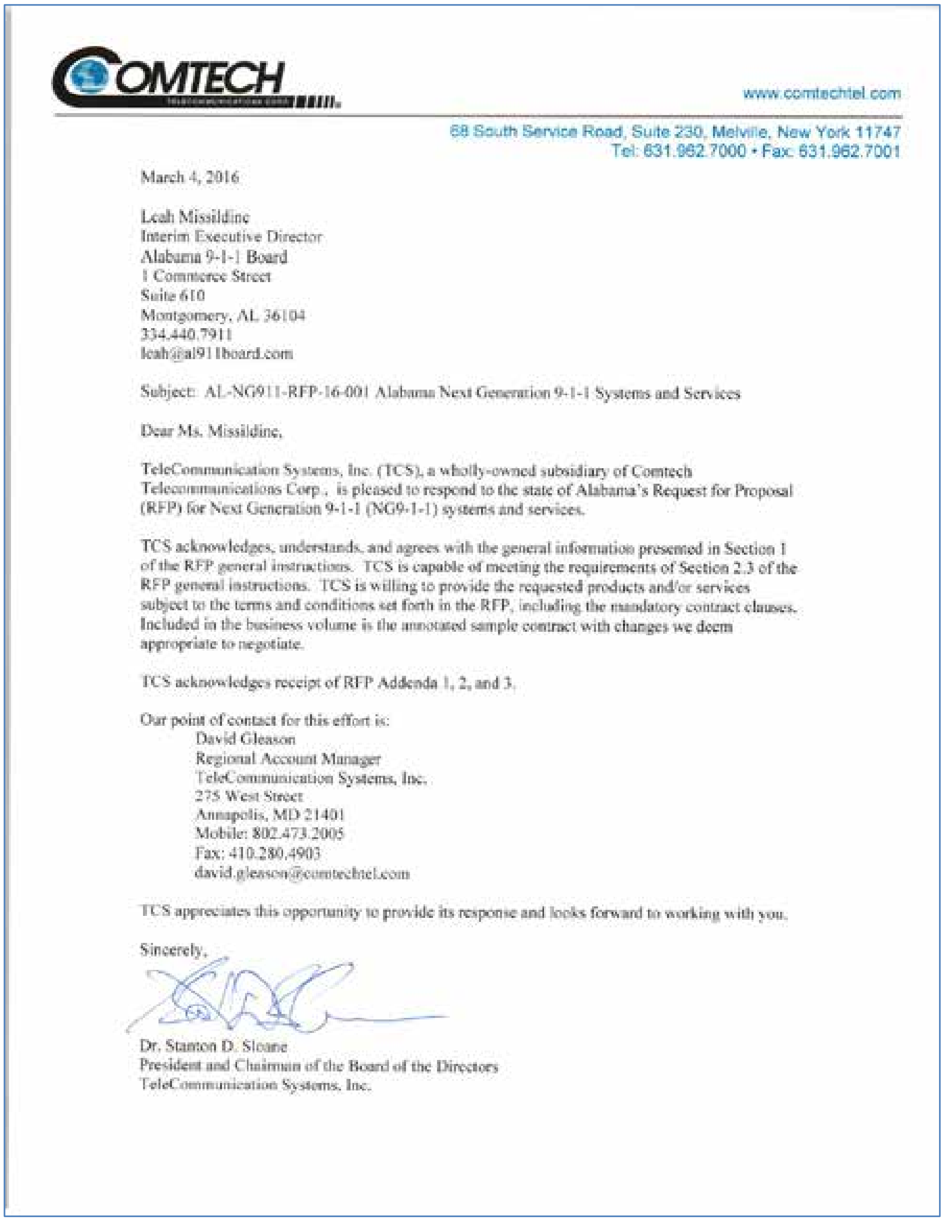
Term	Definition
GUI	Graphical User Interface
HELD	HTTP-Enabled Location Delivery
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBOP	Implementation and Back-Out Plan
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IPS	Intrusion Prevention System
ISDN	Integrated Services Digital Network
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISUP	ISDN User Part
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LbyR	Location by Reference
LbyV	Location by Value
LEC	Local Exchange Carrier
LIF	Location Interwork Function
LIS	Location Information Server
LMR	Land Mobile Radio
LNG	Legacy Network Gateway
LoST	Location to Service Translation
LPG	Legacy PSAP Gateway
LSRG	Legacy Selective Router Gateway

Term	Definition
LTE	Long Term Evolution
LVF	Location Validation Function
MDN	Mobile Directory Number
MF	Multifrequency
MIS	Management Information System
MLP	Mobile Location Protocol
MNS	Managed Network Services
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
NEMA	National Electrical Manufacturers Association
NENA	National Emergency Number Association
NG	Next Generation
NG9-1-1	Next Generation 9-1-1
NGCS	Next Generation Core Services
NG-SEC	NENA 75-001 Security for Next Generation 9-1-1 Standard
NIF	NG9-1-1–Specific Interwork Function
NMS	Network Management System
NOC	Network Operations Center
NTP	Network Time Protocol
NxGnCo	NextGen Communications, Inc.
OGC	Open Geospatial Consortium
OS	Operating System
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
P2P	Peer to Peer

Term	Definition
PAM	PSAP-to-ALI Message
pANI	Pseudo Automatic Number Identification
PBX	Private Branch Exchange
PDU	Power Distribution Unit
PIDF-LO	Presence Information Data Format – Location Object
PIF	Protocol Interwork Function
PMO	Program Management Office
PNL	Preferred Network List
POI	Point of Ingress/Interconnection
POTS	Plain Old Telephone Service
PRF	Policy Routing Function
PRI	Primary Rate Interface
PS/ALI	Private Switch Automatic Location Identification
PSAP	Public Safety Answering Point
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QC	Quality Control
QoS	Quality of Service
RCA	Root Cause Analysis
RFAI	Request for Additional Information
RFC	Request for Comment
RFP	Request for Proposal
RTP	Real-Time Transfer Protocol
SBC	Session Border Controller
SDE	Spatial Database Engine
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIF	Spatial Information Function
SIL	Service Impact Level
SIP	Session Initiation Protocol

Term	Definition
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOI	Service Order Input
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SQL	Structured Query Language
SR	Selective Router
SS7	Signaling System 7
TCC	Text Control Center
TCP	Transmission Control Protocol
TCS	TeleCommunication Systems, Inc.
TDM	Time-Division Multiplexing
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TTY	Teletypewriter
TVSS	Transient Voltage Surge Suppression
UL	Underwriters Laboratories
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UTC	Coordinated Universal Time
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WFS	Web Feature Service
WGS	World Geodetic System
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
XML	Extensible Markup Language

1. Transmittal Letter



COMTECH
TELECOMMUNICATIONS CORP.

www.comtechtel.com

68 South Service Road, Suite 230, Melville, New York 11747
Tel: 631.962.7000 • Fax: 631.962.7001

March 4, 2016

Leah Missildine
Interim Executive Director
Alabama 9-1-1 Board
1 Commerce Street
Suite 610
Montgomery, AL 36104
334.440.7911
leah@al911board.com

Subject: AL-NG911-RFP-16-001 Alabama Next Generation 9-1-1 Systems and Services

Dear Ms. Missildine,

TeleCommunication Systems, Inc. (TCS), a wholly-owned subsidiary of Comtech Telecommunications Corp., is pleased to respond to the state of Alabama's Request for Proposal (RFP) for Next Generation 9-1-1 (NG9-1-1) systems and services.

TCS acknowledges, understands, and agrees with the general information presented in Section 1 of the RFP general instructions. TCS is capable of meeting the requirements of Section 2.3 of the RFP general instructions. TCS is willing to provide the requested products and/or services subject to the terms and conditions set forth in the RFP, including the mandatory contract clauses. Included in the business volume is the annotated sample contract with changes we deem appropriate to negotiate.

TCS acknowledges receipt of RFP Addenda 1, 2, and 3.

Our point of contact for this effort is:
David Gleason
Regional Account Manager
TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401
Mobile: 802.473.2005
Fax: 410.280.4903
david.gleason@comtechtel.com

TCS appreciates this opportunity to provide its response and looks forward to working with you.

Sincerely,

Dr. Stanton D. Sloane
President and Chairman of the Board of the Directors
TeleCommunication Systems, Inc.

2. Executive Summary

2.1. Meeting Alabama's Objectives

The Alabama 9-1-1 Board seeks a statewide Emergency Services Internet Protocol Network (ESInet) to interconnect its 118 Public Safety Answering Points (PSAPs) while leveraging the most benefit from its existing ANGEN Network. TeleCommunication Systems, Inc. (TCS) is pleased to respond to this Request for Proposal (RFP) with a solution that meets this objective.

2.2. Solution Benefits

Alabama's citizens will benefit from a tested, proven, standards-compliant NG9-1-1 system that offers:

- Efficient Internet Protocol (IP)-based call routing, plus the ability to share data among participating entities.
- Deployment of a physically diverse, redundant solution that offers flexibility, expandability, and survivability.
- The ability to process wireline, wireless, and Voice over Internet Protocol (VoIP) calls and to deliver calls through the use of alternative technologies such as text, telemetry, and multimedia.
- A fully redundant system that employs automatic failover so calls will not be lost, and for which manual intervention is not required.
- Cost effectiveness now that extends into the future.

2.3. Solution Components

2.3.1. Base Solution

TCS will install its equipment in the Alabama Supercomputer Authority (ASA) data centers in Huntsville and Montgomery to host the ESInet functional elements. We have designed a highly available Multi-Protocol Label Switching (MPLS) network that has the ability to route calls to all PSAPs, whether they are i3, Request for Additional Information (RFAI), or legacy.

TCS has an entire product line, Intrepid9-1-1™, dedicated to Next Generation 9-1-1 (NG9-1-1) solutions.

Given the unique nature of the existing infrastructure, we have proposed a phased implementation that is made up of a base service plus additional services for later phases. The base service is our core offering of Intrepid9-1-1 Next Generation Core Services (NGCS).

- **Intrepid9-1-1 NGCS –** IP-based selective router (SR) that coordinates call-routing functionality and policy implementation for NG9-1-1 applications, delivering IP-based media to PSAPs regardless of the call source, whether legacy or NG9-1-1. Intrepid9-1-1 is composed of the following National Emergency Number Association (NENA) i3 components as part of the base design: Legacy Network Gateway (LNG)/Legacy Selective Router Gateway (LSRG), Emergency Services Routing Proxy (ESRP) and

Policy Routing Function (PRF), Border Control Function (BCF), and a management information system (MIS) reporting system.

Intrepid9-1-1 NGCS provides all of the components necessary to successfully integrate with the existing ANGEN deployment while providing for increased functionality and availability as compared to the current design. Intrepid9-1-1 NGCS would be deployed in three phases, as follows:

Phase 1: Install LNGs in Huntsville and Montgomery and migrate all existing wireless carrier circuits onto the gateways. While this represents the minimum deployment, we strongly recommend implementing the following two phases as well.

Phase 2: Provision the remainder of the NGCS services to allow for a complete NENA i3 suite of functional elements.

Phase 3: Replace the existing wireless carrier T1 trunks to the SRs with an MPLS mesh network to all PSAPs. Completing this step would allow for an ESInet built on NENA i3 specifications to connect all PSAPs in Alabama. The MPLS network could be built on the ANGEN network if it is suitable; otherwise, a commercial carrier transport network would be procured.

- **EMedia™ –** Enhanced text-to-9-1-1 capability. EMedia enables receipt of Short Message Service (SMS) messages from all carriers over a single interface and provides transfer capability between PSAPs on the EMedia system.
- **Intrepid9-1-1 Automatic Location Identification (ALI) Database Management System (DBMS) –** Our Intrepid9-1-1 ALI product offers full ALI database management for 9-1-1 systems. Our ALI Quality Process Services (AQPS) team will manage current ALI/Master Street Address Guide (MSAG) challenges while preparing for the transition from legacy ALI/MSAG to NG9-1-1. With our Intrepid9-1-1 ALI system, full access to ALI data is provided free of charge.
- **Intrepid9-1-1 ECRF –** As an enhancement to the base Intrepid9-1-1 design, we offer our Emergency Call Routing Function (ECRF) service. The Intrepid9-1-1 ECRF is used for coordinating call routing via NENA i3-compliant ECRF/Location to Service Translation (LoST). Spatial queries use geospatial (x-y) or civic (street address) location information to determine which PSAP should receive a particular call. The service includes Geographic Information System (GIS) updates to the hosted ECRF service.
- **GeoComm Location Validation Function (LVF) –** Consistent with NENA i3 specifications, the LVF will validate location against the geospatial MSAG derived from the master GIS database provided by either the state of Alabama, or as derived from our GIS partners if the state elects that option. The LVF also will use a copy of the same GIS database used by the GeoLynx ECRF. The service includes GIS updates to the hosted LVF service.
- **GIS Spatial Information Function (SIF) Service –** TCS is partnering with GeoComm to manage the GIS data for Intrepid9-1-1 ECRF and the GeoComm LVF functions. GeoComm provides the necessary Quality Assurance (QA)/Quality Control (QC) mechanisms tailored for 9-1-1 GIS data.

- **Emergency Call Tracking System (ECaTS) –** TCS is partnering with Direct Technology to provide reporting tools to meet RFP requirements. This will provide enhanced reporting capability to the state of Alabama.
- **Professional Services –** These services include project management, staging, provisioning, installation, on-site testing, cutover support, and training.
- **Local On-Site Support –** TCS will provide two local technicians for on-site support and to deploy critical replacement spares throughout the network.

2.3.2. Options

This proposal includes the following products and services as options in the pricing:

- **Migration of Wireline Carriers –** Onboarding of existing wireline carriers to the TCS Intrepid9-1-1 NGCS base service. The current infrastructure, where the wireline carriers are delivering calls over Centralized Automatic Message Accounting (CAMA) trunks from the SRs, will be replaced with connections to the aggregation points in the ASA data centers. This would effectively be Phase 4 of the migration to the TCS service at a negotiated additional cost.
- **Cybersecurity Assessment –** TCS will perform a comprehensive security assessment to examine Alabama's ability to endure deliberate, malicious attempts to compromise its network.

2.3.3. Cost Savings

The cost proposal includes key cost savings that Alabama may wish to consider. These include:

- Up to 3 Mbps PSAP network connection
- Removal of GIS based options
- Removal of requirement to deploy a web-based text-9-1-1 browser

2.4. TCS CLEC Subsidiary

To support public safety's adoption of NG9-1-1 and NENA i3 standards and specifications, TCS has invested significant resources in the development of its NENA-compliant NG9-1-1 solution. As a vehicle to channel this focused investment into NG9-1-1, we have created a wholly owned subsidiary called NextGen Communications, Inc. (NxGnCo). NxGnCo is registered and licensed in the state of Alabama as a competitive local exchange carrier (CLEC). Throughout this proposal, the TCS parent company name will be referenced because it is a recognized brand name. However, NxGnCo generally is the contracting entity for the delivery of TCS' innovative NG9-1-1 i3 solutions and systems, and it is expected to be the contracting entity for the system proposed in response to this RFP.

2.5. Valid Pricing Period

Please note that the responses to the requirements in the body of the RFP provide details regarding the features and capabilities of these products. Pricing is valid for a period of 240 days from the proposal opening date.

3. Annotated Sample Contract [RFP Attachment A]

TCS Comment: TCS will work cooperatively with the Board to negotiate mutually agreed upon contractual provision required for compliance with the RFP and our response to it. While we have provided certain comments and suggested revisions to the provisions below, TCS reserves the right to review and negotiate all specific standard or other terms and conditions that the Board wishes to use or incorporate into the definitive contract before entering into such definitive contract. TCS is confident that the parties will be able to negotiate a definitive contract containing terms and conditions that are mutually acceptable to all.

CONTRACT FOR SERVICES

This Contract ("Contract"), entered into by and between the Alabama 911 Board (the "Board") and _________________ (the "Contractor"), is executed pursuant to the terms and conditions set forth herein. In consideration of those mutual undertakings and covenants, the parties agree as follows:

1. Duties of Contractor. The Contractor shall provide the following services relative to this Contract:

[Scope of services to be inserted here and as Appendices/Exhibits upon award of Contract]

2. Consideration. The Contractor shall be compensated for services performed under this Contract as follows:

[Fee information to be inserted upon award of Contract]

3. Term. This Contract shall be effective for a period of [___TBD______]. It shall commence on [__TBD_____] and shall remain in effect through [__TBD______].

4. Access to Records. The Contractor and its subcontractors, if any, shall maintain all books, documents, papers, accounting records, and other evidence pertaining to all costs incurred and payments made under this Contract. Subject to Contractor's and its subcontractors', if any, reasonable security requirements and not more than once every twelve (12) months, they shall make such materials available at their respective offices at all reasonable times during this Contract, and for three (3) years from the date of final payment under this Contract, for inspection by the Board or its authorized designees. Any third party audit would be expected to be conducted by a reputable and nationally recognized audit company. Furthermore, any audit is subject to the representative to whom access to materials is provided being subject to appropriate confidentiality obligations to preclude the disclosure or use of any information except for the purposes of the audit. Such reviews shall take place at a time and place agreed upon by the parties. The Contractor and its subcontractors, if any, may redact from the materials made available for any audit information that reveals the identity or non-public information of other Contractor or subcontractor customers or other Contractor or subcontractor confidential information that is not relevant to the purposes of the audit. Reasonable copies shall be furnished at no cost to the Board if requested.

Deleted: T

Deleted: C

5. Assignment; Successors. The Contractor binds its successors and assignees to all the terms and conditions of this Contract. The Contractor shall not assign or subcontract the whole or any part of this Contract without the Board's prior written consent (which consent shall not be unreasonably withheld). The Contractor may assign its right to receive payments to such third parties as the Contractor may desire without the prior written consent of the Board.

Deleted: , provided that the Contractor gives written notice (including evidence of such assignment) to the Board thirty (30) days in advance of any payment so assigned. The assignment shall cover all unpaid amounts under this Contract and shall not be made to more than one party

6. Assignment of Antitrust Claims. As part of the consideration for the award of this Contract, the Contractor assigns to the Board all right, title and interest in and to any claims the Contractor now has, or may acquire, under state or federal antitrust laws relating to the products or services which are the subject of this Contract.

7. Audits. The Contractor acknowledges that it may be required to submit to an audit of funds paid through this Contract. Any such audit shall be subject to the terms of Section 4 hereof, and shall be conducted in accordance with Chapter 2A, Title 40 Ala. Code, 1975, and audit guidelines reasonably specified by the Board.

The Board considers the Contractor to be a "vendor" for purposes of this Contract. However, if required by applicable provisions of the Office of Management and Budget Circular A-133 (Audits of States, Local Governments, and Non-Profit Organizations) and requested by the Board in writing, following the expiration of this Contract the Contractor shall arrange (at the separate cost and expense of the Board) for a financial and compliance audit of funds provided by the Board pursuant to this Contract. Such audit is to be conducted by an independent public or certified public accountant and performed in accordance with industry best practice and applicable provisions of the Office of Management and Budget Circulars A-133 (Audits of States, Local Governments, and Non-Profit Organizations). The Contractor is responsible for ensuring that the audit and any management letters are completed and forwarded to the Board in accordance with the terms of this Contract. Audits conducted pursuant to this paragraph must be submitted no later than nine (9) months following the close of the Contractor's fiscal year. The Contractor agrees to provide the Board an original of all such financial and compliance audits of funds provided by the Board pursuant to this Contract. The audit shall be an audit of the actual entity, or distinct portion thereof that is the Contractor, and not of a parent, member, or Subsidiary Corporation of the Contractor, except to the extent such an expanded audit may be determined by the Board to be in the best interests of the Board. The audit shall include a statement from the Auditor that the Auditor has reviewed this Contract and that the Contractor is not out of compliance with the financial aspects of this Contract.

8. Authority to Bind Contractor. The signatory for the Contractor represents that he/she has been duly authorized to execute this Contract on behalf of the Contractor and has obtained all necessary or applicable approvals to make this Contract fully binding upon the Contractor when his/her signature is affixed, and accepted by the Board.

9. Changes in Work. The Contractor shall not commence any additional work or change the scope of the work until authorized in writing by the Board. The Contractor shall make no claim for additional compensation in the absence of a prior written approval and amendment executed by all signatories hereto. This Contract may only be amended, supplemented or modified by a written document executed in the same manner as this Contract.

10. Compliance with Laws.

A. The Contractor shall comply with all applicable federal, state, and local laws, rules, regulations, and ordinances, and all provisions required thereby to be included herein are hereby incorporated by reference. The enactment or modification of any applicable state or federal statute or the promulgation of rules or regulations thereunder after execution of this Contract shall be reviewed by the Board and the Contractor to determine whether the provisions of this Contract require formal modification.

B. The Contractor and its agents shall abide by all ethical requirements that apply to persons who have a business relationship with the Board as set forth in The Alabama Ethics Law Sections 36-25-1 et seq. Ala. Code, 1975, as amended and the regulations promulgated thereunder. If the Contractor is not familiar with these ethical requirements, the Contractor should refer any questions to the Alabama State Ethics Commission. If the Contractor or its agents violate any applicable ethical standards, the Board may, in its sole discretion, terminate this Contract immediately upon notice to the Contractor. In addition, the Contractor may be subject to penalties under The Alabama Ethics Law at Section 36-25-27 Ala. Code, 1975, as amended and under any other applicable laws.

C. The Contractor certifies by entering into this Contract that neither it nor its principal(s) is presently in arrears in payment of taxes, permit fees or other statutory, regulatory or judicially required payments to the Board or the State of Alabama. The Contractor agrees that any payments currently due to the Board or the State of Alabama may be withheld from payments due to the Contractor. Additionally, further work or payments may be withheld, delayed, or denied and/or this Contract suspended until the Contractor is current in its payments and has submitted proof of such payment to the Board.

D. The Contractor warrants that it has no current, pending or outstanding criminal, civil, or enforcement actions initiated by the Board or the State of Alabama and agrees that it will immediately notify the Board of any such actions. During the term of such actions, the Contractor agrees that the Board may delay, withhold, or deny work under any supplement, amendment, change order or other contractual device issued pursuant to this Contract.

E. If a valid dispute exists as to the Contractor's liability or guilt in any action initiated by the Board or the State of Alabama or any affiliated agencies, and the Board decides to delay, withhold, or deny work to the Contractor, the Contractor may request that it be allowed to continue, or receive work, without delay. The Contractor must submit, in writing, a request for review to the Board. A determination by the Board shall be binding on the parties. Any payments that the Board may delay, withhold, deny, or apply under this section shall not be subject to penalty or interest.

F. The Contractor warrants that the Contractor and its subcontractors, if any, shall obtain and maintain all required permits, licenses, registrations, and approvals, and shall comply with all health, safety, and environmental statutes, rules, or regulations in the performance of work activities for the Board. Failure to do so may be deemed a material breach of this Contract and grounds for immediate termination and denial of further work with the Board.

G. The Contractor affirms that, Contractor is properly registered and owes no outstanding reports to the Alabama Secretary of State.

11. Condition of Payment. All services provided by the Contractor under this Contract must be performed to the Board's reasonable satisfaction and in accordance with all applicable federal, state, and local laws, ordinances, rules and regulations. The Board shall not be required to pay for work found to be performed in violation of federal, state or local statute, ordinance, rule or regulation.

Deleted: unsatisfactory, inconsistent with this Contract, or

Deleted: and

12. Confidentiality of Board Information. The Contractor understands and agrees that data, materials, and information disclosed to the Contractor by the Board or its agents may contain confidential and protected information. The Contractor covenants that data, material, and information gathered, based upon or disclosed to the Contractor by the Board or its agents for the purpose of this Contract will not be disclosed to or discussed with third parties without the prior written consent of the Board (which consent shall not be unreasonably withheld).

The parties acknowledge that the services to be performed by Contractor for the Board under this Contract may require or allow access to data, materials, and information containing Personally Identifiable Information (defined as any information that identifies or can be used to identify, contact or locate the person to whom such information pertains or from which identification or contact information on an individual can be derived). If any Social Security number(s) is/are disclosed by Contractor in violation of this Contract, Contractor agrees to pay the reasonable cost of the notice of disclosure of a breach of the security of the system in addition to any other claims and expenses for which it is liable under the terms of this contract.

13. Continuity of Services.

A. The Contractor recognizes that the service(s) to be performed under this Contract are vital to the Board and the State of Alabama and must be continued without material interruption and that, upon Contract expiration or termination, a successor, either the Board or another contractor, will need to implement replacement services. During the period until implementation of a successor system the Contractor agrees to (subject to payment by the Board of applicable transition service fees):

Deleted: may continue them

Deleted: T

1. Exercise its commercially reasonable efforts and cooperation to support the Board with effecting an orderly and efficient transition to a successor provider of a replacement service.

Deleted: <#>Furnish phase-in training; and¶

Deleted: best

B. The Contractor shall, upon the Board's written notice (and subject to payment by the Board of applicable transition service fees):

1. Continue to provide services during the transition by the Board to a successor provider of replacement services for up to six (6) months after this Contract is terminated or expires; and

Deleted: period

2. Negotiate in good faith a plan with the Board and any successor provider of replacement services to determine the nature and extent of phase-in, phase-out services necessary to transition operation to such replacement services. The plan shall specify a date for transferring responsibilities for each of the service areas provided to the successor provider of a different service, and shall be subject to the Board's approval (which approval shall not be unreasonably withheld). The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this Contract are maintained at the required level of proficiency.

Deleted: a training program and

C. [Intentionally omitted.]

Deleted: The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this Contract. The Contractor shall also disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

D. The Contractor shall be compensated for reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations).

Deleted: reimbursed

Deleted: Any costs eligible for reimbursement shall not exceed the monthly recurring cost being paid for the services provided under this contract at the time of contract expiration and as approved by the Board.

14. Debarment and Suspension.

A. The Contractor certifies by entering into this Contract that neither it nor its principals nor any of its subcontractors are presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from entering into this Contract by any federal agency or by any department, agency or political subdivision of the State of Alabama. The term "principal" for purposes of this Contract means an officer, director, owner, partner, key employee or other person with primary management or supervisory responsibilities, or a person who has a critical influence on or substantive control over the operations of the Contractor.

B. The Contractor certifies that it has used reasonable efforts to verify the state and federal suspension and debarment status for all subcontractors receiving funds from it under this Contract and, as between Contractor and the Board, it shall be responsible for any recoupment, penalties or reasonable costs that might arise from use of a suspended or debarred subcontractor. The Contractor shall promptly notify the Board if it becomes aware that any subcontractor under this Contract becomes debarred or suspended during the term of this Contract, and shall, at the Board's request, take all reasonable steps required by the Board to terminate its contractual relationship with the subcontractor for work to be performed under this Contract.

Deleted: ied

Deleted: solely

Deleted: immediately

15. Default by Board. If the Board, within sixty (60) days after receipt of written notice, fails to correct or cure any material breach of this Contract, in addition to and not in lieu of any other rights, remedies or damages, the Contractor may cancel and terminate this Contract and institute measures to collect monies due up to and including the date of termination.

Deleted: ninety (90)

16. Disputes.

A. Should any disputes arise with respect to this Contract, the Contractor and the Board agree to act promptly to attempt to resolve such disputes. Time is of the essence in the resolution of disputes.

Deleted: immediately

B. Each party agrees that, the existence of a dispute notwithstanding, it will continue without delay to carry out all of its responsibilities under this Contract that are not affected by the dispute. Should the either party fail to continue to perform its responsibilities regarding all non-disputed work, without delay, any additional costs incurred as a result of such failure to proceed shall be borne by the non-performing party, and the non-performing party shall make no claim against the other for such costs.

Deleted: The Contractor

Deleted: Contractor

Deleted: by the Board or the Contractor

Deleted: Contractor

Deleted: Contractor

Deleted: Board

C. If a party to the Contract is not satisfied with the progress toward resolving a dispute, the party must notify in writing the other party of this dissatisfaction. Upon written notice, the parties have ten (10) working days, unless the parties mutually agree to extend this period, following the notification to resolve the dispute. If the dispute is not resolved within ten (10) working days, the parties shall submit the dispute, in compliance with the recommendations to the Attorney General, when considering settlement of such disputes, to utilize appropriate forms of alternate dispute resolution, including, but not limited to, mediation by or through the Attorney General's Office of Administrative Hearing or where appropriate, private mediators. If a party if not satisfied with the results of mediation, the dissatisfied party may submit the dispute to the Circuit Court of Montgomery County, Alabama.

D. The Board may withhold payments on disputed items pending resolution of the dispute; provided, however, that in no event shall objection by the Board to any part of any invoice be cause to delay acceptance and/or payment on any undisputed portion of any invoice. The unintentional nonpayment by the Board to the Contractor of one or more invoices not in dispute in accordance with the terms of this Contract will not be cause for the Contractor to terminate this Contract except in accordance with Section 15.

E. It is agreed that the terms and commitments contained herein shall not be constituted a debt of the State of Alabama in violation of Article XI, Section 213, of the Constitution of Alabama, 1901, as amended by Amendment No. 26. It is further agreed that if any provision of this contract shall contravene any statute or constitutional provision or amendment, either now in effect or which may, during the course of this contract, be enacted, then that conflicting provision of the contract shall be deemed to be modified to the extent necessary to allow it to be enforced to the extent permitted by applicable law, or if it cannot be so modified, the offending provision, or part thereof, shall be deemed severed from the Contract. In any event, the remaining provisions of this Contract shall remain in full force and effect.

Deleted: null and void

17. Drug-Free Workplace Certification. The Contractor hereby covenants and agrees to make a good faith effort to provide and maintain a drug-free workplace. The Contractor will give written notice to the Board within ten (10) days after receiving actual notice that the Contractor, or an employee of the Contractor in the State of Alabama, has been convicted of a criminal drug violation occurring in the workplace. False certification or violation of this certification may result in sanctions including, but not limited to, suspension of contract payments, termination of this Contract and/or debarment of contracting opportunities with the Board for up to three (3) years.

In addition to the provisions of the above paragraph, if the total amount set forth in this Contract is in excess of $25,000.00, the Contractor certifies and agrees that it will provide a drug-free workplace by:

A. Publishing and providing to all of its employees a statement notifying them that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the Contractor's workplace, and specifying the actions that will be taken against employees for violations of such prohibition;

B. Establishing a drug-free awareness program to inform its employees of (1) the dangers of drug abuse in the workplace; (2) the Contractor's policy of maintaining a drug-free workplace; (3) any available drug counseling, rehabilitation and employee assistance programs; and (4) the penalties that may be imposed upon an employee for drug abuse violations occurring in the workplace;

C. Notifying all employees in the statement required by subparagraph (A) above that as a condition of continued employment, the employee will (1) abide by the terms of the statement; and (2) notify the Contractor of any criminal drug statute conviction for a violation occurring in the workplace no later than five (5) days after such conviction;

D. Notifying the Board in writing within ten (10) days after receiving notice from an employee under subdivision (C)(2) above, or otherwise receiving actual notice of such conviction;

E. Within thirty (30) days after receiving notice under subdivision (C)(2) above of a conviction, imposing the following sanctions or remedial measures on any employee who is convicted of drug abuse violations occurring in the workplace: (1) taking appropriate personnel action against the employee, up to and including termination; or (2) requiring such employee to satisfactorily participate in a drug abuse assistance or rehabilitation program approved for such purposes by a federal, state or local health, law enforcement, or other appropriate agency; and

F. Making a good faith effort to maintain a drug-free workplace through the implementation of subparagraphs (A) through (E) above.

18. Employment Eligibility Verification. As required by Alabama state law, the Contractor swears or affirms under the penalties of perjury that the Contractor does not knowingly employ an unauthorized alien. The Contractor further agrees that:

A. The Contractor shall enroll in and verify the work eligibility status of all his/her/its newly hired employees through the E-Verify program as defined in IC §22-5-1.7-3. The Contractor is not required to participate should the E-Verify program cease to exist. Additionally, the Contractor is not required to participate if the Contractor is self-employed and does not employ any employees.

B. The Contractor shall not knowingly employ or contract with an unauthorized alien. The Contractor shall not retain an employee or contract with a person that the Contractor subsequently learns is an unauthorized alien.

C. The Contractor shall require his/her/its subcontractors, who perform work under this Contract, to certify to the Contractor that the subcontractor does not knowingly employ or contract with an unauthorized alien and that the subcontractor has enrolled and is participating in the E-Verify program. The Contractor agrees to maintain this certification throughout the duration of the term of a contract with a subcontractor.

The Board may terminate for default if the Contractor fails to cure a breach of this provision no later than thirty (30) days after being notified by the Board.

19. [Intentionally omitted.]

Deleted: Employment Option. If the Board determines that it would be in the Board's best interest to hire an employee of the Contractor, the Contractor will release the selected employee from any non-competition agreements that may be in effect. This release will be at no cost to the Board or the employee.

20. Force Majeure. In the event that either party is unable to perform any of its obligations under this Contract or to enjoy any of its benefits because of natural disaster or decrees of governmental bodies or other cause that is not the fault of the affected party (hereinafter referred to as a "Force Majeure Event"), the party who has been so affected shall promptly give notice to the other party and shall do everything commercially reasonable to resume performance as soon as reasonably practicable. Upon receipt of such notice, all obligations under this Contract shall be immediately suspended. If the period of nonperformance exceeds thirty (30) days from the receipt of notice of the Force Majeure Event, the party whose ability to perform has not been so affected may, by giving written notice, terminate this Contract.

Deleted: immediately

Deleted: possible

21. Funding Cancellation. When the Board makes a written determination that funds are not authorized by statute or otherwise available to support continuation of performance of this Contract, this Contract shall be canceled. A determination by the Board that funds are not authorized or otherwise available to support continuation of performance shall be final and conclusive.

22. Governing Law. This Contract shall be governed, construed, and enforced in accordance with the laws of the State of Alabama, without regard to its conflict of laws rules. Suit, if any, must be brought in the Circuit Court of Montgomery County, Alabama.

23. Indemnification. The Contractor agrees to indemnify, defend, and hold harmless the Board, its agents, officials, and employees from all claims and suits including court costs, attorney's fees, and other expenses caused by any act or omission of the Contractor and/or its subcontractors, if any, in the performance of this Contract. The Board shall not provide such indemnification to the Contractor.

24. Independent Contractor; Workers' Compensation Insurance. The Contractor is performing as an independent entity under this Contract. No part of this Contract shall be construed to represent the creation of an employment, agency, partnership or joint venture agreement between the parties. Neither party will assume liability for any injury (including death) to any persons, or damage to any property, arising out of the acts or omissions of the agents, employees or subcontractors of the other party. The Contractor shall provide all necessary unemployment and workers' compensation insurance for the Contractor's employees, and shall provide the Board with a Certificate of Insurance evidencing such coverage prior to starting work under this Contract.

25. Insurance.

Deleted: The Contractor shall secure and keep in force during the term of this Contract the following insurance coverage, covering the Contractor for any and all claims of any nature which may in any manner arise out of or result from Contractor's performance under this Contract:

A. The Contractor and their subcontractors (if any) shall secure and keep in force during the term of this Contract the following insurance coverages (if applicable) covering the Contractor for any and all claims of any nature which may in any manner arise out of or result from Contractor's performance under this Contract:

1. Commercial general liability, including contractual coverage, and products or completed operations coverage (if applicable), with minimum liability limits not less than $5,000,000 per occurrence unless additional coverage is required. The Board is to be named as an additional insured on a primary, non-contributory basis for any liability arising directly or indirectly under or in connection with this Contract.

Deleted: $700,000 per person and

2. Automobile liability for owned, non-owned and hired autos with minimum liability limits of $5,000,000 per accident. The Board is to be named as an additional insured on a primary, non-contributory basis.

Deleted: $700,000 per person and

Deleted: occurrence

3. Professional Liability, also known as Errors and Omissions Insurance, for those Contractors required to hold a professional license in Alabama with limits not less than $700,000 per cause of action and $5,000,000 per occurrence. This is coverage available to pay for liability arising out of the performance of professional or business related duties, with coverage tailored to the needs of the specific profession.

Deleted: Coverage for the benefit of the Board shall continue for a period of two (2) years after the date of service provided under this Contract.

4. Fiduciary Liability would be required if the Contractor is responsible for the management and oversight of various employee benefit plans and programs such as pensions, profit-sharing and savings, among others. These contractors face potential claims for mismanagement brought by plan members. Limits should be no less than $700,000 per cause of action and $5,000,000 per occurrence.

5. Valuable Papers coverage, available under an Inland Marine policy, is recommended when any plans, drawings, media, data, records, reports, billings and other documents are produced or used under this agreement. Insurance must have limits sufficient to pay for the re-creation and reconstruction of such records.

6. [The Contractor shall secure the appropriate Surety or Fidelity Bond(s) as required by applicable statutes.]

TCS Comment: TCS is providing a hosted service and, therefore, does not believe such project should be considered a "public works" necessitating any bonding. To the extent any form of performance assurance is required, TCS will agree to negotiate with the Board to determine an appropriate and mutually acceptable form of reasonable performance assurance. It is TCS' expectation that the Board would be responsible for any costs associated with obtaining any mutually agreed upon form of performance assurance and TCS would be able to separately invoice and be compensated for any such costs,

7. The Contractor shall provide proof of such insurance coverage by tendering to the Board a certificate of insurance prior to the commencement of this Contract and proof of workers' compensation coverage meeting all statutory requirements. In addition, proof of an "all states endorsement" covering claims occurring outside Alabama is required if any of the services provided under this Contract involve work outside of Alabama.

B. The Contractor's insurance coverage must meet the following additional requirements:

1. The insurer must have a certificate of authority or other appropriate authorization to operate in the state in which the policy was issued.

2. Any deductible or self-insured retention amount or other similar obligation under the insurance policies shall be the sole obligation of the Contractor.

3. The Board will be defended, indemnified and held harmless to the full extent of any coverage actually secured by the Contractor in excess of the minimum requirements set forth above. The duty to indemnify the Board under this Contract shall not be limited by the insurance required in this Contract.

4. The insurance required in this Contract, through a policy or endorsement(s), shall include a provision that the policy and endorsements may not be canceled or modified without thirty (30) days' prior written notice to the Board.

5. The Contractor waives and agrees to require their insurer to waive their rights of subrogation against the Board.

C. Failure to provide insurance as required in this Contract may be deemed a material breach of contract entitling the Board to immediately terminate this Contract in accordance with Section 43. The Contractor shall furnish a certificate of insurance and all endorsements to the Board before the commencement of this Contract.

26. [Intentionally omitted.].

27. Minority, Women, and Veteran Business Enterprise Participation. Substantially all of the work under this Contract will be performed directly by the Contractor's employees or by its certified technicians. Prior to the time the Contractor employs any third party subcontractors, the Contractor will work with the Board to identify opportunities and select qualified participants.

28. Licensing Standards. The Contractor, its employees and subcontractors shall comply with all applicable licensing standards, certification standards, accrediting standards and any other laws, rules, or regulations governing services to be provided by the Contractor pursuant to this Contract. If any required license, certification or accreditation expires or is revoked, or any disciplinary action is taken against an

Deleted: **Key Person(s)**

Deleted: A. If both parties have designated that certain individual(s) are essential to the services offered, the parties agree that should such individual(s) leave their employment during the term of this Contract for whatever reason, the Board shall have the right to terminate this Contract upon thirty (30) days' prior written notice.¶
¶
B. In the event that the Contractor is an individual, that individual shall be considered a key person and, as such, essential to this Contract. Substitution of another for the Contractor shall not be permitted without express written consent of the Board.¶
¶
Nothing in sections A and B, above shall be construed to prevent the Contractor from using the services of others to perform tasks ancillary to those tasks which directly require the expertise of the key person. Examples of such ancillary tasks include secretarial, clerical, and common labor duties. The Contractor shall, at all times, remain responsible for the performance of all necessary tasks, whether performed by a key person or others.¶
¶
Key person(s) to this Contract is/are ____¶

Deleted: The Board will not pay the Contractor for any services performed when the Contractor, its employees or subcontractors are not in compliance with such applicable standards, laws, rules, or regulations.

applicable license, certification, or accreditation, the Contractor shall notify the Board promptly and the Board, at its option, may terminate this Contract in accordance with Section 43.

Deleted: immediately

Deleted: immediately

29. Merger & Modification. This Contract constitutes the entire agreement between the parties. No understandings, agreements, or representations, oral or written, not specified within this Contract will be valid provisions of this Contract. This Contract may not be modified, supplemented, or amended, except by written agreement signed by all necessary parties.

30. Nondiscrimination.

Pursuant to the federal Civil Rights Act of 1964, the Age Discrimination in Employment Act, and the Americans with Disabilities Act, the Contractor covenants that it shall not discriminate against any employee or applicant for employment relating to this Contract with respect to the hire, tenure, terms, conditions or privileges of employment or any matter directly or indirectly related to employment, because of the employee's or applicant's race, color, national origin, religion, sex, age, disability, ancestry, status as a veteran, or any other characteristic protected by federal, state, or local law ("Protected Characteristics"). Contractor certifies compliance with applicable federal laws, regulations, and executive orders prohibiting discrimination based on the Protected Characteristics in the provision of services. Breach of this paragraph may be regarded as a material breach of this Contract, but nothing in this paragraph shall be construed to imply or establish an employment relationship between the Board and any applicant or employee of the Contractor or any subcontractor.

The Board is periodically a recipient of federal funds, and therefore, where applicable, Contractor and any subcontractors shall comply with requisite affirmative action requirements, including reporting, pursuant to 41 CFR Chapter 60, as amended, and Section 202 of Executive Order 11246.

31. Notice to Parties. Whenever any notice, statement or other communication is required under this Contract, it shall be sent by first class mail or via an established courier or delivery service to the following addresses, unless otherwise specifically advised.

A. Notices to the Board shall be sent to:

Alabama 911 Board
Attn: ______________________________________
[ADDRESS]

B. Notices to the Contractor shall be sent to: **(Include contact name and/or title, name of vendor & address)**

____

____

____

____

Payments to the Contractor shall be made via electronic funds transfer in accordance with instructions filed by the Contractor with the Board. Either party may change its address for notices upon delivery of notice as required by this Section.

32. Order of Precedence; Incorporation by Reference. Any irreconcilable inconsistency or ambiguity in this Contract shall be resolved by giving precedence in the following order: (1) this Contract, including its Exhibits/Appendices otherwise expressly referenced in this Contract, (2) Contractor's response to RFP#_____, and (3) RFP#_____. All attachments, and all documents referred to in this paragraph, are hereby incorporated fully by reference.

Deleted: attachments prepared by the Board, (3) RFP#_____, (4)

Deleted: 5

Deleted: attachments prepared by the Contractor

33. Ownership of Documents and Materials. All documents, records, programs, data, film, tape, articles, memoranda, and other materials not developed or licensed by the Contractor prior to execution of this Contract, but specifically developed under this Contract shall be considered "work for hire" and the Contractor transfers any ownership claim to the Board and all such materials will be the property of the Board. Use of these materials, other than related to contract performance by the Contractor, without the prior written consent of the Board, is prohibited. During the performance of this Contract, the Contractor shall be responsible for any loss of or damage to these materials developed for or supplied by the Board and used to develop or assist in the services provided while the materials are in the possession of the Contractor. Any loss or damage thereto shall be restored at the Contractor's expense. The Contractor shall provide the Board full, immediate, and unrestricted access to the work product during the term of this Contract.

34. Payments. All payments shall be made 60 days in arrears by electronic funds transfer to the financial institution designated by the Contractor in writing. No payments will be made in advance of receipt of the goods or services that are the subject of this Contract.

35. Penalties/Interest/Attorney's Fees. The Board will in good faith perform its required obligations hereunder and does not agree to pay any penalties, liquidated damages, interest or attorney's fees, except as permitted by Alabama law.

Any liability resulting from the Board's failure to make prompt payment shall be based solely on the amount of funding originating from the Board and shall not be based on funding from federal or other sources (but only to the extent such funding from federal other sources has not actually been received by the Board).

36. Progress Reports. The Contractor shall submit progress reports to the Board upon reasonable request. The progress reports shall serve the purpose of assuring the Board that work is progressing in line with the schedule, and that completion can be reasonably assured on the scheduled date.

37. Public Record. The Contractor acknowledges that the Board will not treat this Contract as containing confidential information (provided that any trade secrets identified by Contractor may be protected as such from any open records request to the extent provided by applicable law). Use by the public of the information contained in this Contract shall not be considered an act of the Board.

38. Renewal Option. This Contract may be renewed under the same terms and conditions, subject to the approval of the Board and mutual written agreement of Contractor. The term of the renewed contract may not be longer than the term of the original contract.

39. Severability. The invalidity of any section, subsection, clause or provision of this Contract shall not affect the validity of the remaining sections, subsections, clauses or provisions of this Contract.

40. Substantial Performance. This Contract shall be deemed to be substantially performed only when fully performed according to its terms and conditions and any written amendments or supplements.

41. Taxes. Any and all fees specified in this Contract do not include sales, use, property, value-added, withholding or other taxes, duties or fees, associated with the licenses granted or Products or Services provided in this Contract ("Taxes"). The Board is exempt from most state and local taxes and many federal taxes. Unless to the Board provides necessary information to Contractor and a valid tax exemption certificate, Taxes shall be the responsibility of the Board and will be billed to and paid by the Board; provided however, that this Section shall in any event not apply to Taxes based on Contractor's net income or payroll, Except as provided above, the Board will not be responsible for any taxes levied on the Contractor as a result of this Contract.

Deleted: T

42. Termination for Convenience. This Contract may be terminated, in whole or in part, by the Board whenever, for any reason, the Board determines that such termination is in its best interest. Termination of services shall be effected by delivery to the Contractor of a Termination Notice at least thirty (30) days prior to the termination effective date, specifying the extent to which performance of services under such termination becomes effective. The Contractor shall be compensated for services properly rendered prior to the effective date of termination. The Board will not be liable for services performed after the effective date of termination. The Contractor shall be compensated for services herein provided but in no case shall total payment made to the Contractor exceed the original contract price or shall any price increase be allowed on individual line items if canceled only in part prior to the original termination date.

43. Termination for Default.

A. With the provision of thirty (30) days' notice to the Contractor, the Board may terminate this Contract in whole or in part if the Contractor fails to:

1. Correct or cure any breach of a material provision of this Contract that is identified with particularity in the written notice from the Board; provided the time to correct or cure the breach

may be extended beyond thirty (30) days if the Board determines progress is being made and the extension is agreed to by the parties; or

2. Correct or cure any breach of any of the other provisions of this Contract that is identified with particularity in the written notice from the Board; provided the time to correct or cure the breach shall be not less than sixty (60) days unless the Board determines progress is being made and a further extension is agreed to by the parties.

Deleted: Deliver the supplies or perform the services within the time specified in this Contract or any extension;¶
3. Make progress so as to endanger performance of this Contract; or¶
4. Perform

B. [Intentionally omitted.]

Deleted: If the Board terminates this Contract in whole or in part, it may acquire, under the terms and in the manner the Board considers appropriate, supplies or services similar to those terminated, and the Contractor will be liable to the Board for any excess costs for those supplies or services. However, the Contractor shall continue the work not terminated.

C. The Board shall pay the contract price for completed supplies delivered and services accepted. The Contractor and the Board shall agree on the amount of payment for manufacturing materials delivered and accepted and for the protection and preservation of the property. Failure to agree will be a dispute under the Disputes clause.

Deleted: The Board may withhold from these amounts any sum the Board determines to be necessary to protect the Board against loss because of outstanding liens or claims of former lien holders.

D. The rights and remedies of the Board in this clause are in addition to any other rights and remedies provided by law or equity or under this Contract.

44. Effect of Termination. Termination of the Contract shall not limit either party from pursuing other remedies available to it, including injunctive relief, nor shall such termination relieve the Board of its obligation to pay all fees that have accrued under the Contract prior to termination of the Contract (and. Notwithstanding anything to the contrary in this Contract, including any early termination fees incurred by Contractor with respect to any third parties). Upon termination of the Contract (i) the Board's right to use any of the materials and services provided by Contractor shall immediately terminate; and (ii) upon Contractor's request, the Board shall return any deliverables in its possession or control to Contractor. Upon termination of the Contract, the Board furthermore, at the request of the Contractor, shall promptly certify that it has destroyed or returned to the Contractor all of the Contractor's confidential or proprietary information, and all copies or derivatives in any form thereof, whether or not modified or merged into other materials.

45. License. For greater certainty, and notwithstanding anything to the contrary in this Contract, it is understood and agreed that the Contractor is only granting to the Board a limited, nontransferable and nonexclusive license to use the materials and services provided by the Contractor hereunder (the "System") for internal purposes during the term of this Contract. The license granted under this Contract to use the System extends to the Board's employees and the PSAP employees authorized by the Board to use the System (collectively, "Internal Users") for the permitted purposes described above. Each Internal User's use of the System shall be subject to all of the terms and conditions of the Contract and the Board shall be responsible to Contractor for the failure of any Internal User to comply with any terms or conditions of the Contract. The Board will not (nor permit any Internal User or third party not authorized by Contractor to) modify, enhance, translate, reverse engineer, decompile, disassemble or attempt to reconstruct, identify or discover any source code, underlying ideas or algorithms of the System or any other form of Contractor's intellectual property, disassemble or decompile any part of the System, nor cause, permit, or attempt any of the foregoing. The Board shall not create (nor permit any Internal User or third party not authorized by Contractor to create) any derivative works based upon the System or any of its components. In furtherance and not limitation of the foregoing, and notwithstanding anything else to the contrary in this Contract, as between the Board and the Contractor, title to all hardware and other communications equipment installed by the Contractor in connection with the System will remain with the Contractor. As between the Board and the Contractor, title to all software provided by the Contractor and used by the Board or the Contractor in connection with the System will remain at all times with the Contractor. The Board acknowledges that except for the license expressly granted to the Board under this Section 45 to use the System all other intellectual property rights (in whatever form) in and to the System and any other development efforts hereunder in relation thereto are and will remain the property of the Contractor.

46. **Travel**. No expenses for travel will be reimbursed unless specifically permitted under the scope of services or consideration provisions. If approved by the Board, expenditures made by the Contractor for travel will be reimbursed at the current rate paid by the Board and in accordance with the State Travel Policies and Procedures as specified in the current Financial Management Circular. Out-of-state travel requests must be reviewed by the Board for availability of funds and for appropriateness per Circular guidelines.

47. **Waiver of Rights**. No right conferred on either party under this Contract shall be deemed waived, and no breach of this Contract excused, unless such waiver is in writing and signed by the party claimed to have waived such right. Neither the Board's review, approval or acceptance of, nor payment for, the services required under this Contract shall be construed to operate as a waiver of any rights under this Contract or of any cause of action arising out of the performance of this Contract.

Deleted: 45

Deleted: , and the Contractor shall be and remain liable to the Board in accordance with applicable law for all damages to the Board caused by the Contractor's negligent performance of any of the services furnished under this Contract

48. Warranty.

Deleted: 46

Deleted: **Work Standards**. The Contractor shall execute its responsibilities by following and applying at all times the highest professional and technical guidelines and standards. If the Board becomes dissatisfied with the work product of or the working relationship with those individuals assigned to work on this Contract, the Board may request in writing the replacement of any or all such individuals, and the Contractor shall grant such request.

A. **Services Warranty.** Contractor warrants to the Board that the services provided by Contractor hereunder shall, at the time of acceptance and for a period of thirty (30) days thereafter, (a) be performed by Contractor in a manner consistent with generally accepted professional standards and (b) conform in all material respects to their applicable specifications as provided herein.

B. **Exclusions from Warranty.** The above warranties for services shall be void to the extent that defects or failures of the services to conform with applicable specifications are caused by (a) the Board's or any end user's negligence, misuse, or accident; (b) any alteration by the Board or any end user not approved by Contractor; or (c) problems relating to or caused by software, materials or services (including, without limitation, any installation services) not provided or approved by Contractor. Furthermore, Contractor is not responsible for conditions outside its reasonable control. Additional fees (including, without limitation, applicable hourly professional or other fees at Contractor's then-applicable standard rates and any other out-of-pocket expenses) may be charged by Contractor for any repairs, revisions or replacements to services made by Contractor resulting from defects or failures not covered by the above warranties.

C. **Remedy for Breach of Warranty.** If any covered services fail to conform to their applicable warranty set forth above, and the Board notifies Contractor of such nonconformance in writing within the applicable warranty period, the Board's exclusive remedy and Contractor's entire liability shall be for Contractor, at its option, (a) to the extent reasonably possible, repair, revise, re-perform or replace the defective or non-conforming services to bring the same into compliance with their applicable warranty above; or (ii) in the event the remedy specified in (i) is not accomplished in a reasonable period of time or is not reasonably possible, refund to the Board the pro-rated amount actually paid by the Board to Contractor for the relevant defective or non-conforming services. Any replacement or re-performed services provided will be warranted from the date of replacement or re-performance for thirty (30) days in accordance with the terms of this Section.

D. **Disclaimers**. Except as provided in Section 48.A above, Contractor does not warrant that (i) the services will meet the Board's requirements, (ii) the services will operate in combination with other hardware, software, systems or data not provided or validated by Contractor that the Board or any end user may select for use, or (iii) the operation of services will be uninterrupted or error-free. Without limiting any of the foregoing, Contractor shall not be responsible for the quality or accuracy of any data not originally developed by it, nor shall Contractor be responsible for any errors or other issues in the operation or delivery of services resulting from, in whole or in part, any data not originally developed by it or any other matter outside of its reasonable control.

EXCEPT AS OTHERWISE EXPRESSLY SET FORTH IN THIS SECTION 48, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SERVICES (INCLUDING ALL CONTENT, SOFTWARE, FUNCTIONS, MATERIALS, INFORMATION AND EQUIPMENT INCLUDED OR PROVIDED BY CONTRACTOR OR ANY OTHER THIRD PARTY IN CONNECTION THEREWITH) ARE PROVIDED AS IS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY WARRANTIES IMPLIED OR REQUIRED BY LAW THAT CANNOT BE DISCLAIMED ARE LIMITED IN DURATION TO A WARRANTY PERIOD OF THIRTY (30) DAYS FROM ORIGINAL ACCEPTANCE OF THE COVERED SERVICES. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, CONTRACTOR DISCLAIMS ANY AND ALL LIABILITY ARISING FROM ANY MISUSE OR UNAUTHORIZED DISCLOSURE OF DATA FROM THE SERVICES BY THE BOARD, ANY END USERS OR ANY OTHER THIRD PARTY.

49. 911 Service Provider Protections. No provisions of this Contract shall be construed as affecting or negating the standards or limitations for liability set forth in any applicable law limiting the liability of any party providing or assisting in providing any 911-related products or services.

50. Limitation of Liability. IN NO EVENT SHALL CONTRACTOR'S AGGREGATE LIABILITY TO THE BOARD UNDER THE TERMS OF THE CONTRACT EXCEED THE TOTAL PAYMENTS ACTUALLY RECEIVED BY CONTRACTOR FROM THE BOARD PURSUANT TO OR IN CONNECTION WITH THE CONTRACT IN THE PRECEDING TWELVE-MONTH PERIOD. IN NO EVENT SHALL CONTRACTOR BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY THE BOARD OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF TCS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITHOUT LIMITING THE FOREGOING, TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ANY OF CONTRACTOR'S LICENSORS BE LIABLE FOR ANY DAMAGES OR LOSS OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF

PROFITS, REVENUE, DATA OR USE, INCURRED BY THE BOARD OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SUCH LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. The provisions of the Contract allocate the risks between Contractor and the Board. The Board acknowledges and agrees that the pricing it received for the services hereunder reflects this allocation of risk and the limitation of liability specified herein.

51. Appropriation Efforts. Notwithstanding anything to the contrary in this Contract, the Board agrees to continue to use good faith efforts to secure such appropriations or other expenditure authority as may be necessary to pay Contractor for the services under this Contract throughout the term of this Contract. The Board furthermore agrees to provide Contractor with written notice of any non-appropriation or other limitation of funding not less than sixty (60) days in advance of the last day of the date when funding for the services based on then existing appropriations, limitations, or other expenditure authority would be spent.

52. Board Notification of Indemnity Claims. The Board shall provide Contractor with prompt written notice of any claim for which indemnification is sought hereunder. The parties thereafter shall work together in good faith to manage the defense, settlement or compromise of such claim. The Board agrees not to incur expenses nor settle or compromise any claim for which indemnification is sought under this Contract without the prior written consent of the Contractor (which consent shall not be unreasonably withheld or delayed).

53. Publicity. No press releases or other public disclosures of or relating to this Agreement shall be made by either Party without the prior mutual written consent of the Parties unless required by law or regulatory authority. Customer consents to the use of Customer's commercial name in TCS's customer and/or partner lists. TCS may disclose the existence of this Master Sales Agreement and any Statement of Work to its service providers for forecast purposes.

54. Counterparts. This Contract may be executed simultaneously in one or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. The exchange of a fully executed Contract (in counterparts or otherwise) by facsimile shall be sufficient to bind the parties to the terms and conditions of this Contract.

Non-Collusion and Acceptance

The undersigned attests, subject to the penalties for perjury, that the undersigned is the Contractor, or that the undersigned is the properly authorized representative, agent, member or officer of the Contractor. Further, to the undersigned's knowledge, neither the undersigned nor any other member, employee (other than internal employees whose compensation may be based on sales commissions), representative, agent or officer of the Contractor, directly or indirectly, has entered into or been offered any sum of money or other consideration for the execution of this Contract other than that which appears upon the face hereof.

In Witness Whereof, Contractor and the Board have, through their duly authorized representatives, entered into this Contract. The parties, having read and understood the foregoing terms of this Contract, do by their respective signatures dated below agree to the terms thereof.

[Contractor]	Alabama Statewide 911 Board
By: ____________________________________	By: __________________________________
Printed Name: ___________________________	Printed Name: ________________________
Title: __________________________________	Title: _________________________________
Date: __________________________________	Date: _________________________________

4. Business Proposal Spreadsheet [RFP Attachment B]

A completed business proposal spreadsheet is included in this submission. Below are the accompanying attachments required in RFP Attachment B.

4.1. Respondent's Company Structure [RFP 2.3.2]

4.1.1. TCS Company Leadership

TCS operates as a wholly owned subsidiary of Comtech Telecommunications Corp. (NASDAQ: CMTL or "Comtech"). Information about Comtech's management team and board of directors is accessible on the Comtech website at www.comtechtel.com/manage.cfm. Lynne Houserman serves as President of Comtech's Safety and Security Technologies group (of which TCS now is a part).

4.1.2. Safety and Security Technologies Leadership

The Alabama ESInet will be managed by Comtech TCS Safety and Security Technologies, as shown in Exhibit 1.

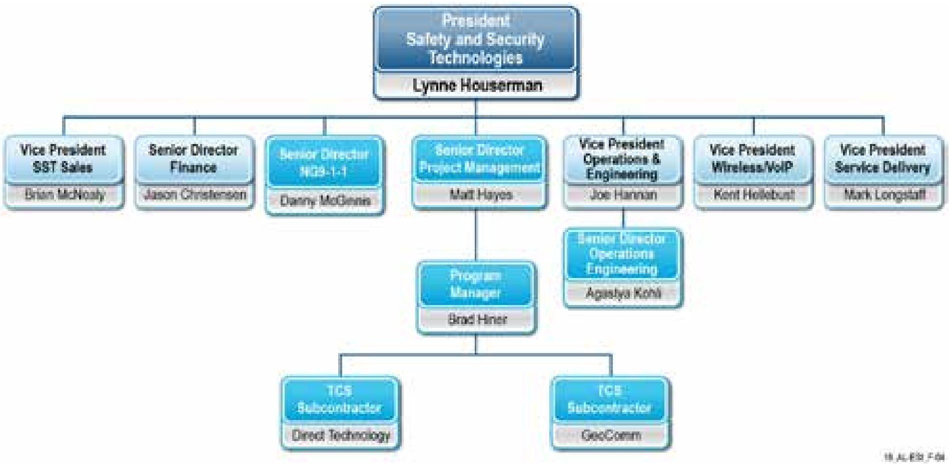
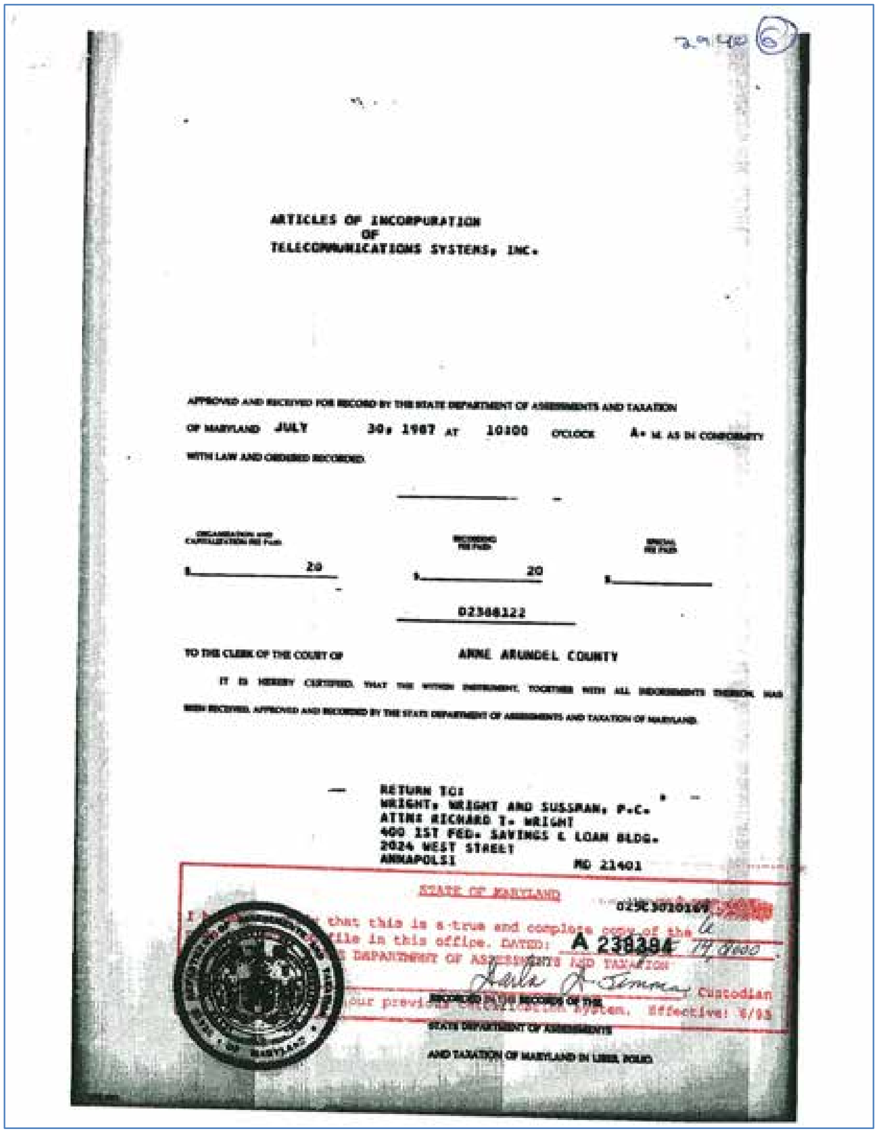


Exhibit 1. Safety and Security Technologies Organizational Chart

Lynne Houserman leads the Safety and Security Technologies group. Reporting to her is Matt Hayes, Senior Director, Project Management. Reporting to Matt is Brad Hiner, the Program Manager dedicated to the Alabama ESInet deployment. Brad will manage the other TCS personnel assigned to the project from TCS systems engineering team, which includes personnel responsible for network provisioning, equipment staging/provisioning, equipment installation, testing, and cutover and end-user training. Reporting to Vice President of Operations & Engineering Joe Hannan is Agastya Kohli, who will provide the engineering support for the project. Danny McGinnis will manage the program for contract years beyond initial implementation. Mark Longstaff oversees the TCS NOC and monitoring teams.

4.1.3. Certificate of Authority

Exhibit 2 shows TCS' "Articles of Incorporation" for the State of Maryland in which the company was formed.



29140 6

ARTICLES OF INCORPORATION
OF
TELECOMMUNICATIONS SYSTEMS, INC.

APPROVED AND RECEIVED FOR RECORD BY THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION OF MARYLAND JULY 30, 1987 AT 10:00 O'CLOCK A. M. AS IN CONFORMITY WITH LAW AND ORDERED RECORDED.

ORGANIZATION AND CAPITALIZATION FEE PAID	RECORDING FEE PAID	SPECIAL FEE PAID
$ 20	$ 20	$

02388122

TO THE CLERK OF THE COURT OF ANNE ARUNDEL COUNTY

IT IS HEREBY CERTIFIED, THAT THE WITHIN INSTRUMENT, TOGETHER WITH ALL INDORSEMENTS THEREON, HAS BEEN RECEIVED, APPROVED AND RECORDED BY THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION OF MARYLAND.

RETURN TO:
WRIGHT, WRIGHT AND SUSSMAN, P.C.
ATTN: RICHARD T. WRIGHT
400 1ST FED. SAVINGS & LOAN BLDG.
2024 WEST STREET
ANNAPOLIS, MD 21401

STATE OF MARYLAND

02SC3010169

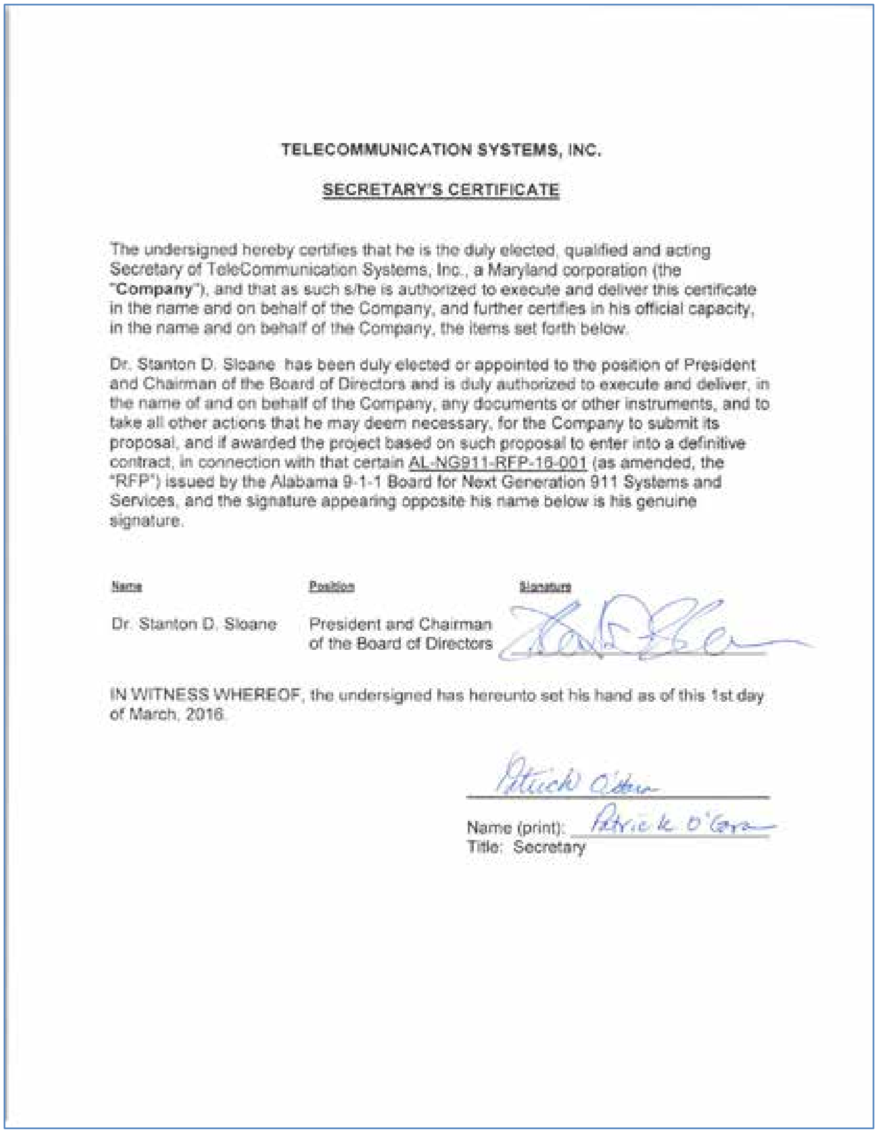
I [illegible] that this is a true and complete copy of the [illegible] file in this office. DATED: A 238394 [illegible] 14, 2000
[illegible] DEPARTMENT OF ASSESSMENTS AND TAXATION
Karla J. Simmons Custodian
[illegible] our previous certification system. Effective: 6/95

RECORDED IN THE RECORDS OF THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION OF MARYLAND IN LIBER, FOLIO

Exhibit 2. Certificate of Authority

4.2. Authorizing Document [RFP 2.3.8]

Exhibit 3 shows TCS' "Secretary's Certificate" that proves Dr. Stanton D. Sloane's authority to sign the proposal transmittal letter.



TELECOMMUNICATION SYSTEMS, INC.

SECRETARY'S CERTIFICATE

The undersigned hereby certifies that he is the duly elected, qualified and acting Secretary of TeleCommunication Systems, Inc., a Maryland corporation (the "**Company**"), and that as such s/he is authorized to execute and deliver this certificate in the name and on behalf of the Company, and further certifies in his official capacity, in the name and on behalf of the Company, the items set forth below.

Dr. Stanton D. Sloane has been duly elected or appointed to the position of President and Chairman of the Board of Directors and is duly authorized to execute and deliver, in the name of and on behalf of the Company, any documents or other instruments, and to take all other actions that he may deem necessary, for the Company to submit its proposal, and if awarded the project based on such proposal to enter into a definitive contract, in connection with that certain AL-NG911-RFP-16-001 (as amended, the "RFP") issued by the Alabama 9-1-1 Board for Next Generation 911 Systems and Services, and the signature appearing opposite his name below is his genuine signature.

Name	Position	Signature
Dr. Stanton D. Sloane	President and Chairman of the Board of Directors	

IN WITNESS WHEREOF, the undersigned has hereunto set his hand as of this 1st day of March, 2016.

Patrick O'Gara

Name (print): Patrick O'Gara
Title: Secretary

Exhibit 3. Authorizing Document

4.3. Subcontractors [RFP 2.3.9]

4.3.1. Direct Technology

A. Each subcontractor's name, address, and state of incorporation that are proposed to be used in providing the required products and services

Subcontractor name: ECaTS, a division of Direct Technology Inc. Corporate Headquarters: 3009 Douglas Blvd., Suite 300, Roseville, CA 95661. State of incorporation: Washington

B. Each subcontractor's area(s) of responsibility under the proposal

The ECaTS MIS and Analytics group is recognized as subject matter experts in reporting and Public Safety Intelligence and proposes to provide the first universal 911 Call Reporting System in response (specifically) to the System Reporting and i3 Logging Requirements, Section 5, of RFP AL-NG911-RFP-16-001 Attachment D Technical Specifications

C. The anticipated dollar amount for each subcontract

Please see pricing volume for costs.

D. Each subcontractor's form of organization

Corporation

E. An indication from each subcontractor of a willingness to carry out their responsibilities (this assurance in no way relieves the Respondent of any responsibilities in responding to this RFP or in completing the commitments documented in this proposal)

ECaTS, a division of Direct Technology and a subcontractor on this proposal, is willing to provide applicable requested products and/or services subject to the terms and conditions set forth in the RFP including, but not limited to, mandatory contract clauses.

F. The qualifications of each subcontractor for guaranteeing performance

ECaTS, a division of Direct Technology, is a team of professionals with a proven track record in public safety analytics since 1997, specifically in the aggregation and reporting of 9-1-1 statistics for more than 1,200 PSAPs across the country. ECaTS MIS and Analytics service is currently installed and in production statewide throughout California, Utah, Oregon, North Carolina, parts of Texas, Florida, Kentucky, Mississippi, Montana, Tennessee, Oklahoma, and Washington.

G. Identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience in the technical proposal for each portion of the proposed products or services to be provided by the subcontractor

Reporting and Data Collection – ECaTS is an MIS and analytics company that has been involved in public safety for 19 years. ECaTS has partnered with several Customer Premise Equipment (CPE) vendors and service providers throughout the country to deliver statewide, regional, and local reporting and analytics solutions.

Statewide Statistical Monitoring – ECaTS is already providing or in the process of providing statewide statistical monitoring for several states.

Operational Reporting and Logging – ECaTS is qualified to provide an i3-compliant logging service interface which aggregates logs from the network (e.g., an ESInet) and the call-handing system to support end-to-end transaction logging and retrieval. The ECaTS logger web services conforms to NENA 8-003 v1 Detailed Functional and Interface Specification for the NENA i3 Solution, Stage 3 Version 1. Currently ECaTS provides multiple methodologies for interoperability from direct physical interfaces to more complex logical interfaces that leverage the i3 standards for collection, recording, and storage of i3 events

H. Any other data that may be required by the State

None.

4.3.2. GeoComm

A. Each subcontractor's name, address, and state of incorporation that are proposed to be used in providing the required products and services

Name: GeoComm, Inc.

Address: 601 W. Saint Germain St., St. Cloud, MN 56301

State of Incorporation: Minnesota

B. Each subcontractor's area(s) of responsibility under the proposal

4.3 Emergency Call Routing Function (ECRF)

4.8 Location Validation Function (LVF)

C. The anticipated dollar amount for each subcontract

Please see pricing volume for costs.

D. Each subcontractor's form of organization

GeoComm was acquired in May 2013 by Granite Equity Partners (GEP), a Minnesota-based private investment firm. GEP is registered with the Securities and Exchange Commission and detailed information about GEP is available on the SEC’s website.

E. An indication from each subcontractor of a willingness to carry out their responsibilities (this assurance in no way relieves the Respondent of any responsibilities in responding to this RFP or in completing the commitments documented in this proposal)

GeoComm has read, understands, and will comply with the RFP requirements as described throughout the response documents submitted with this proposal.

F. The qualifications of each subcontractor for guaranteeing performance

GeoComm is an Esri Platinum Partner, a leading innovator on Esri technology mapping the future of NG9-1-1. Over the past several years, GeoComm has become a proven provider of end-to-end GIS systems tailored to meet the needs of public safety agencies moving to NG9-1-1. GeoComm offers NG9-1-1 specific software and services, including NG9-1-1 GIS data assessment and development; GIS workflow consulting; software to maintain, manage, and provision NG9-1-1 GIS data; the ECRF/LVF elements of the ESInet; and tactical mapping for emergency responders and PSAPs. GeoComm’s GeoLynx family of products provides the tools necessary to geospatially route 9-1-1 calls, speed and enhance emergency response, improve data accuracy and quality, accelerate communications, and provide mission-critical GIS-based decision support.

Types of Customers

GeoComm's GIS and software services have been provided to a growing number of clients nationally, including the states of Maine, New York, Vermont, North Dakota, South Dakota, Iowa, and Texas; the 11-county region surrounding Washington, DC; the nine-county area surrounding Kansas City governed by the Mid-America Regional Council (MARC); the large metropolitan area of Lee County, Florida (Fort Myers); the 22-PSAP 9-1-1 jurisdiction governed by the Association of Central Oklahoma Governments (ACOG); the Denver metropolitan area governed by Jefferson County and Broomfield, Colorado; the greater Dallas-Fort Worth area under the 9-1-1 authority of North Central Texas Council of Governments (NCTCOG); and 20 U.S. military installations.

GIS Experience and Qualifications

GeoComm's GIS Services Bureau has the largest professional public safety GIS staff in the nation. These staff members are dedicated to ensuring the GIS data developed and maintained is of the highest quality and meets standards embraced by the 9-1-1 industry. GeoComm works with a wide range of customers possessing varying levels of GIS and public safety knowledge, personnel, and technical environments. GeoComm's GIS Services Bureau has developed more than 4.65 million addresses and developed more than 417,000 road miles for public safety agencies nationwide. The company provides all-inclusive GIS services tailored to implementing GIS data in Enhanced 9-1-1 (E9-1-1) and NG9-1-1 environments, including:

- GIS data synchronization analysis
- GIS map data development and enhancements
- GPS field collection and verification
- Road centerline
- Address points
- Emergency service area boundaries
- Community boundaries
- GIS map data maintenance
- NG9-1-1 QC and ongoing provisioning services
- MSAG and ALI database development

Public Safety GIS Applications

GeoComm, one of 12 Esri Platinum Partners worldwide and the only public safety Platinum Partner, has a unique understanding of how to maximize the value GIS can bring to public safety. GeoComm develops software products for quickly accessing needed GIS data, viewing map data, and editing regional data sets efficiently. GeoComm has been at the forefront of integrating GIS into public safety software products for years. The products GeoComm offers are considered "best of breed" in the public safety industry. Its GeoLynx family of products includes:

- GeoLynx Server Tactical PSAP Mapping
- Vehicle tracking (AVL)
- Statistical querying (Stats)
- FEMA Integrated Public Alert and Warning System
- GeoLynx Mobile Server Edition
- GeoLynx Desktop Tactical PSAP Mapping
- GeoLynx Mobile Tactical Responder Mapping
- GeoLynx Mobile MDC Edition
- GeoLynx Mobile Server Edition
- Enterprise Public Safety GIS Data Management
- GeoLynx DMS for desktop data management
- GeoLynx Server Web DMS for online web editing
- GeoLynx Server GIS Change Requests for data contributors
- GeoLynx Server GIS Portal
- NG9-1-1 GIS System Provisioning
- GeoLynx Spatial Router i3 ECRF and LVF

Public Safety GIS and Project Management Services

GeoComm's project management team provides exceptional, client-specific GIS integration advising and project management services to assist public safety agencies in making informed decisions for developing and/or improving GIS services for their communities. This team is composed of industry-recognized professionals and subject matter experts who have successfully completed various projects across the country. GeoComm listens objectively to the goals and requirements of each client's specific project. Then, the company outlines customized recommendations and practical implementation steps to meet the client's project goals.

GeoComm partners with its clients to provide expertise and knowledge as it relates to their project. The company specializes in GIS public safety services for all levels of public safety agencies, including:

- Maintenance workflow
- NG9-1-1 data report card
- NG9-1-1 GIS transition management
- Project management

G. Identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience in the technical proposal for each portion of the proposed products or services to be provided by the subcontractor

Please see responses to B and F, above.

H. Any other data that may be required by the State

None.

4.4. General Information [RFP 2.3.10]

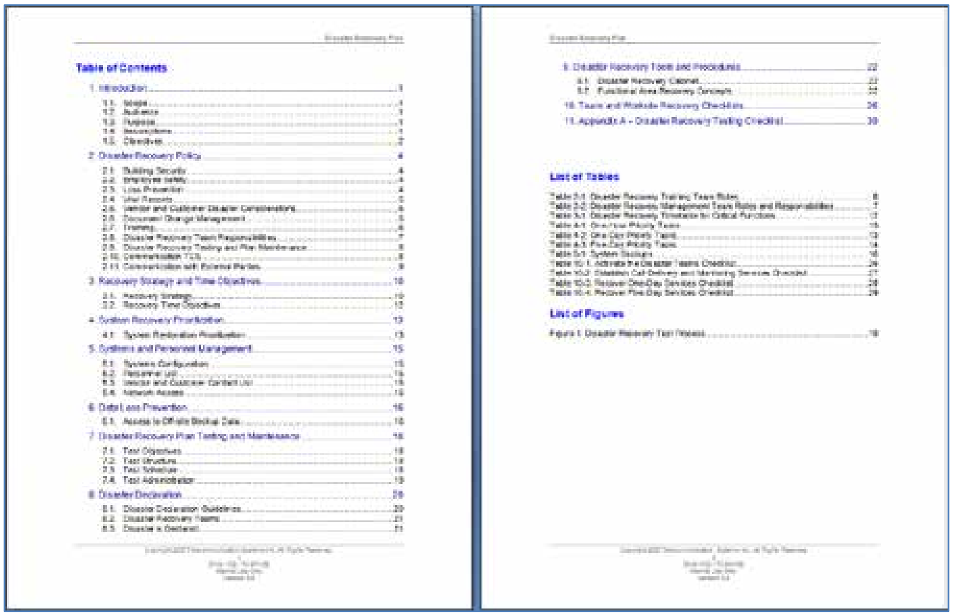
TCS will present a disaster recovery plan to Alabama for approval. This plan will be invoked in the event of a catastrophic failure of all, or a significant portion of, the 9-1-1 service, and will allow for the substantial time to repair or to mitigate the adverse impact to public safety.

As part of our International Organization for Standardization (ISO) and TL certifications, we have established our internal disaster recovery plan, fully tested our plan, update our plan quarterly, and practice it on a regular basis.

We will include fundamental aspects of the documentation and practice such as:

- A discussion of possible risks to the data centers, equipment, data, and processes.
- A program to manage potential risks by eliminating them or reducing them to an acceptable level.
- A strategy to recover from threats that cannot be eliminated but can be foreseen.
- Reviews of the various risks and instructions for specific systems recovery.

TCS is highly qualified to transfer its established skills, and TCS carries forward these competencies in documenting, preparing, and testing to handle potential disasters on behalf of the State. The disaster recovery plan is proprietary information, so it is excluded from this proposal. Instead, we offer Exhibit 4, which depicts the table of contents of our disaster recovery plan.



Disaster Recovery Plan

Table of Contents

1 Introduction ... 1
1.1. Scope ... 1
1.2. Audience ... 1
1.3. Purpose ... 1
1.4. Assumptions ... 1
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 Offsite 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

[illegible]

Disaster Recovery Plan

9. Disaster Recovery Tools and Procedures ... 22
9.1. Disaster Recovery Cabinet ... 22
9.2. Functional Area Recovery Concepts ... 22
10. Team and Worksite Recovery Checklists ... 26
11. Appendix A – Disaster Recovery Testing Checklist ... 30

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 5-1: 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 ... 18

[illegible]

Exhibit 4. Table of Contents from TCS' Established Disaster Recovery Plan

Part of the disaster recovery effort will be to determine if the existing T1 connections to the legacy SRs are a viable, and valuable, addition to recovery efforts. Barring effective utilization of the existing T1 circuits, we would then look to commercial carrier backup networks, wireless networks, satellite, or other tertiary means to re-establish connectivity. The availability of any of these items is dependent on necessary bandwidth, site location, and a number of other site-specific criteria that can be discussed with the State in detail. For consideration, we note that wireless Long Term Evolution (LTE) backup appears to be the preferred option in other deployments with which we are familiar.

AL-NG911-RFP-16-001 Next Generation 911 Systems and Services

Attachment B - Business Proposal

Instructions

Tab Name	Instructions
Business Proposal	Please fill in the cells shaded yellow and indicate if any attachments are included in the response to each item. Some items require a yes/no answer and an explanation if the answer is no.

AL-NG911-RFP-16-001 ATTACHMENT B - BUSINESS PROPOSAL

Respondent Name:	**TeleCommunication Systems, Inc.**
	Please Complete Yellow Shaded Regions

2.3.1 GENERAL (OPTIONAL)

Enter your response below. Please indicate if attachments are included.

The Respondent may use this optional section of the business proposal to introduce or summarize any information the Respondent deems relevant or important to the State's successful acquisition of the products and/or services requested in this RFP.	Known for engineering and delivering highly reliable wireless communications technology, TeleCommunication Systems, Inc. (TCS) enables the life-saving transmission of voice, video, and data information. Whether providing a highly secure communications link in remote places, connecting people to emergency services, or pioneering new messaging and location-based services and applications, helping people make "Connections that Matter"® is what TCS does best. As a leading provider of mission-critical wireless data solutions to government customers, public safety providers, and wireless communications carriers, TCS develops wireless data technology designed to handle the need for both security and reliability. Since completing the first U.S. wireless Enhanced 9-1-1 (E9-1-1) solution in 1997, TCS has been leading the way in public safety solutions for wireless E9-1-1, NG9-1-1, and the European emergency telephone number, E1-1-2. The company is also pioneering and improving the methods by which U.S. PSAPs can receive a wireless or VoIP subscriber's location during calls for emergency assistance. In March 1998, the company was the first to deploy commercial wireless E9-1-1 Phase I service as defined in Federal Communications Commission (FCC) Report and Order 94 102, before the Phase I mandate was in effect. TCS deployed Phase II service beginning in April 2002 and has offered VoIP i2 E9-1-1 service since 2005, developing what has become the National Emergency Number Association (NENA) standard for the current generation of VoIP E9-1-1. Today, TCS supports half of all U.S. wireless E9-1-1 calls. Its award-winning wireline, wireless, and VoIP E9-1-1 solutions serve more than 140 million wireless and IP-enabled devices, ensuring that a subscriber's emergency call routes to the appropriate PSAP and that the caller's location information is provided.

2.3.2 RESPONDENT'S COMPANY STRUCTURE

Enter your response below. Please indicate if attachments are included.

The legal form of the Respondent's business organization, the state in which formed (accompanied by a certificate of authority), the types of business ventures in which the organization is involved, and a chart of the organization are to be included in this section. If the organization includes more than one product division, the division responsible for the development and marketing of the requested products and/or services in the United States must be described in more detail than other components of the organization.	TCS is a corporation formed in Maryland that serves the telecommunication industry and both its commercial and government customers. Organization charts and a certificate of authority are included in the attachment.

2.3.3 COMPANY FINANCIAL INFORMATION

Enter your response below. Please indicate if attachments are included.

This section must include the Respondent's financial statement, including an income statement and balance sheet, for each of the two most recently completed fiscal years. The financial statements must demonstrate the Respondent's financial stability. If the financial statements being provided by the Respondent are those of a parent or holding company, additional financial information should be provided for the entity/organization directly responding to this RFP.	TCS' revenue for the first quarter of 2015 was $81.9 million, 4 percent less than 2014's first quarter figures. Revenue for the second quarter of 2015 was $87.9 million, up 7 percent from the previous quarter and up 2 percent from the second quarter of 2014. Revenue for the third quarter was $101.1 million, up 15 percent from the previous quarter and up 6 percent from the third quarter of 2014. In 2014, TCS reported revenue of $359.9 million. Revenue for the first quarter of 2014 was $85.1 million, up 8 percent sequentially from the previous quarter. Revenue for the second quarter of 2014 was $86.2 million. Revenue for the third quarter of 2014 was $95.3 million, up 11 percent compared to the previous quarter. Revenue for the fourth quarter of 2014 was $93.3 million. In 2013, TCS reported revenue of $362.3 million. Revenue for the first quarter of 2013 was $94.8 million, down 5% from Q1 2012. Revenue for the second quarter of 2013 was $92.8 million, down 19% from Q2 2012. Revenue for the third quarter of 2013 was $96 million, up 3% sequentially from the previous quarter and down 31% from Q3 2012. Revenue for the fourth quarter of 2013 was $79 million. In 2012, TCS reported revenue of $487.4 million. Revenue for the first quarter of 2012 was $100 million, up 11% from Q1 2011. Revenue for the second quarter of 2012 was $114.6 million, up 14% from Q2 2011. Revenue for the third quarter of 2012 was $140.1 million, up 24% from Q3 2011. Revenue for the fourth quarter of 2012 was $132.7 million, up 9% from Q4 2011. In 2011, TCS reported revenue of $425.4 million. Revenue for the first quarter of 2011 was $90.4 million as compared to $90.9 million Q1 2010. Revenue for the second quarter of 2011 was $100.7 million, up 9% from Q2 2010. Revenue for the third quarter of 2011 was $112.6 million, up 9% from Q3 2010. Revenue for the fourth quarter of 2011 was $121.7 million, up 19% from Q4 2010. TCS' DUNS Number is 19-697-0503 for its Annapolis, Maryland, facility; and 62-723-4198 for its Tampa, Florida, facility. TCS is a publicly traded company. All company SEC filings are accessible on the TCS website at www.telecomsys.com under Investors > Financial Information > SEC Filings.

2.3.4 INTEGRITY OF COMPANY STRUCTURE AND FINANCIAL REPORTING

This section must include a statement indicating that the CEO and/or CFO has taken personal responsibility for the thoroughness and correctness of any and all financial information supplied with this proposal. The particular areas of interest to the Board in considering corporate responsibility include the following items: separation of audit functions from corporate boards and board members, if any, the manner in which the firm assures board integrity, and the separation of audit functions and consulting services. The State of Alabama will consider the information offered in this section to determine the responsibility of the Respondent.

The Sarbanes Oxley Act of 2002, H.R. 3763, is NOT directly applicable to this procurement; however, its goals and objectives may be used as a guide in the determination of corporate responsibility for financial reports.

Enter your response below. Please indicate if attachments are included.

TCS is a publicly traded company. TCS has implemented both GAAP and SOX accounting controls to ensure that our financial reporting is in accordance with SEC requirements. In addition, each periodic financial report containing financial statements filed with the SEC is accompanied by a written statement by the CEO and CFO (i.e., Section 906 certification) that information contained in the periodic report fairly presents, in all material respects, the Company's financial condition and results of operations. TCS financial reporting, controls, processes and procedures are audited annually by our internal and external auditors to ensure that we are in compliance with GAAP and SOX. All company SEC filings are accessible on the TCS website at www.telecomsys.com under Investors > Financial Information > SEC Filings.

Internal Audit at TCS is an independent, objective assurance and consulting activity, which reports functionally to the Audit Committee (i.e., for strategic direction, reinforcement, and accountability) and administratively to the CFO (i.e., for assistance in establishing direction, support, and administrative interface). The Internal Audit Director meets privately at least once every fiscal quarter, with the Audit Committee, has direct access to the Audit Committee, and can take directly to the Chair of the Audit Committee, any matter that is believed to be of sufficient magnitude and importance to require immediate attention of the Audit Committee.

2.3.5 CONTRACT TERMS/CLAUSES

The contract resulting from this RFP will contain both mandatory and non-mandatory clauses. Mandatory clauses are non-negotiable while non-mandatory clauses are highly desirable. **Attachment A** contains a sample contract that will be similar to the one resulting from this RFP. Please indicate your acceptance of the following mandatory/non-mandatory clauses within the sample contract. If a non-mandatory clause is not acceptable as worded, please indicate in the "Additional Contract Considerations" and suggest a specific alternative wording to address issues raised by the specific clause in the explanation space provided.
To reiterate, it's the Board's strong desire to not deviate from the contract provided in the attachment and as such the Board reserves the right to reject any and all of these requested changes. Failure to include a clear, specific, unequivocal agreement to these clauses may result in disqualification of the proposal from further evaluation.

Mandatory Clauses	Acceptance? (Yes / No)	If No, Explanation
Duties of Contractor, Rate of Pay, and Term of Contract	Yes	
Authority to Bind Contractor	Yes	
Compliance with Laws	Yes	
Drug-free Workplace Provision and Certification	Yes	
Employment Eligibility Verification	Yes	
Funding Cancellation	Yes	
Governing Laws	Yes	
Indemnification	Yes	
Information Technology	Yes	
Non-discrimination Clause	Yes	
Ownership of Documents and Materials	Yes	
Payments	Yes	
Penalties/Interest/Attorney's Fees	Yes	
Termination for Convenience	Yes	
Non-collusion and Acceptance	Yes	

Enter your response below. Please indicate if attachments are included.

Additional Contract Considerations
Please note: *The Board will only review or negotiate changes to contract clauses clearly identified in the transmittal letter. If there are no contract clauses identified, Respondent is considered to have accepted the clauses as they are currently written.*

Please see annotated sample contract for recommended changes of the non-mandatory contract clauses.

2.3.6 REFERENCES

The Respondent must include a list of at least three (3) clients for whom the Respondent has provided products and/or services that are the same or similar to those products and/or services requested in this RFP. Any state government for whom the Respondent has provided these products and services should be included; also to be included should be clients with locations near Alabama as site visits may be arranged. Information provided should include the name, address, and telephone number of the client facility and the name, title, and phone/fax numbers of a person who may be contacted for further information.

Reference One

Enter your response below.

Legal Name of Company or Governmental Entity	**Tennessee Emergency Communications Board**
Industry of Company	**Public Safety**
Mailing Address	**500 James Robertson Parkway, Davy Crockett Tower, Nashville, TN 37243**
Telephone Number	**615-253-2164**
Contact Name	**Curtis Sutton**
Title	**Executive Director**
Telephone/Fax Number	**615-253-2164**
E-mail Address	**Curtis.Sutton@tn.gov**
Time period in which services were provided	**January 2012-present**
Please describe the service provided to this reference	**TCS direct contract with TECB: TCS has been contracted to provide Professional Services to support the NG9-1-1 over NetTN Program Implementation. These services include program and project management, change management, and service management. In addition to professional services, TCS also provides a 24x7 Tier 1 Network Operations Center serving all Tennessee 9-1-1 centers. TCS is also implementing a hosted Administrative ALI service, currently planned for first integration in Q1 2016. TCS as subcontractor for AT&T: TCS is providing professional services, material, i3-compliant call routing software, ALI database software, training and support to AT&T for the 9-1-1 Over Network Tennessee (NetTN) project. This multi-year project's goal is to migrate more than 160 primary and secondary PSAPs to a NENA i3-compliant, IP-based and spatial call routing system over a State-owned ESInet.**

Reference Two

Enter your response below.

Legal Name of Company or Governmental Entity	**North Central Texas Council of Governments (NCTCOG)**
Industry of Company	**Public Safety**
Mailing Address	**616 Six Flags Drive, Arlington, TX 76005**
Telephone Number	**817-695-9218**
Contact Name	**Mark Brown**
Title	**Chief 9-1-1 Program Officer**
Telephone/Fax Number	**817-695-9218**
E-mail Address	**mbrown@nctcog.org**
Time period in which services were provided	**July 2013-present**
Please describe the service provided to this reference	**NCTCOG is a voluntary organization of, by and for local governments, serving 16 counties in the Dallas-Fort Worth metropolitan area. Fourteen counties participate in the E9-1-1 program, which provides service to 44 public safety answering points. TCS provides ESInet and NG9-1-1 network systems and services, including Legacy Network Gateway (LNG), Legacy Selective Router Gateway (LSRG), GIS-based ECRF, GIS services and Legacy PSAP Gateway (LPG). TCS also provides the network connectivity, managing an MPLS core network and the connections to the PSAPs. TCS provides 24x7 Network Operations Center (NOC) services to the COG and PSAPs.**

Reference Three

Enter your response below.

Legal Name of Company or Governmental Entity	**Iowa Homeland Security and Emergency Management Department**
Industry of Company	**Public Safety**
Mailing Address	**6800 NW 78th Ave Bldg 1, Floor Basement, Johnston, IA 50131**
Telephone Number	**515-323-4232**
Contact Name	**Blake DeRouchey**
Title	**E911 Program Manager**
Telephone/Fax Number	**515-323-4232**
E-mail Address	**blake.derouchey@iowa.gov**
Time period in which services were provided	**April 2012-present**

Please describe the service provided to this reference	**TCS provides a statewide NG9-1-1 network for the routing and delivery of wireless 9-1-1 calls to 119 PSAPs serving over three million people. Network component systems are owned by the State, with connectivity provided by a state agency (ICN). TCS provided the Legacy Network Gateways for ingress from the wireless carriers and custom-built Legacy PSAP Gateways for egress to the PSAPs. These custom units enable the legacy PSAP equipment to answer wireless calls via the NG network and wireline calls via the legacy E9-1-1 network. As PSAPS upgrade to IP enabled call handling systems, the network is adjusted to deliver wireless calls via SIP. TCS manages the network for the State, providing maintenance, monitoring, technical support, and professional services.**

Please identify all references for the past five (5) years for whom your company has provided the same or similar services as those requested in this RFP, but the contract was terminated for cause or for convenience.

Reference One

	Enter your response below.
Legal Name of Company or Governmental Entity	**None.**
Industry of Company	
Mailing Address	
Telephone Number	
Contact Name	
Title	
Telephone/Fax Number	
E-mail Address	
Time period in which services were provided	
Please describe the service provided to this reference	
Provide reason(s) for loss or termination	

Reference Two

	Enter your response below.
Legal Name of Company or Governmental Entity	**None.**
Industry of Company	
Mailing Address	
Telephone Number	
Contact Name	
Title	
Telephone/Fax Number	
E-mail Address	
Time period in which services were provided	
Please describe the service provided to this reference	
Provide reason(s) for loss or termination	

Reference Three

	Enter your response below.
Legal Name of Company or Governmental Entity	**None.**
Industry of Company	
Mailing Address	
Telephone Number	
Contact Name	
Title	
Telephone/Fax Number	
E-mail Address	
Time period in which services were provided	
Please describe the service provided to this reference	
Provide reason(s) for loss or termination	

Corporate Litigation

	Enter your response below. Please indicate if attachments are included.
Does your company have any pending litigation regarding contract disputes?	**None**

2.3.7 REGISTRATION TO DO BUSINESS

	Registered? (Yes / No)	**If No, Explanation**

Respondents providing the products and/or services required by this RFP must be registered and in good standing with the Alabama Secretary of State. The requirement is applicable to all limited liability partnerships, limited partnerships, corporations, S-corporations, nonprofit corporations, and limited liability companies. Please indicate the status of registration.	**Yes**	

2.3.8 AUTHORIZING DOCUMENT

	Enter your response below. Please indicate if attachments are included.
Respondent personnel signing the Transmittal Letter of the proposal must be legally authorized by the organization to commit the organization contractually. This section shall contain proof of such authority. A copy of corporate bylaws or a corporate resolution adopted by the board of directors indicating this authority will fulfill this	Please see Section 4.2 [RFP 2.3.8] in the business proposal for signature authority.

2.3.9 SUBCONTRACTORS

	Enter your response below. Please indicate if attachments are included.
The Respondent is responsible for the performance of any obligations that may result from this RFP, and shall not be relieved by the non-performance of any subcontractor. Any Respondent's proposal must identify all subcontractors and describe the contractual relationship between the Respondent and each subcontractor. Either a copy of the executed subcontract or a letter of agreement over the official signature of the firms involved must accompany each proposal. Any subcontracts entered into by the Respondent must be in compliance with all State statutes, and will be subject to the provisions thereof. For each portion of the proposed products or services to be provided by a subcontractor, the technical proposal must include the identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience. The combined qualifications and experience of the Respondent and any or all subcontractors will be considered in the Board's evaluation. The Respondent must furnish information to the Board as to the amount of the subcontract, the qualifications of the subcontractor for guaranteeing performance, and any other data that may be required by the State. All subcontracts held by the Respondent must be made available upon request for inspection and examination by appropriate Board officials, and such relationships must meet with the approval of the Board. The Respondent must furnish the following information for their use of subcontractors: A. Each subcontractor's name, address, and state of incorporation that are proposed to be used in providing the required products and services B. Each subcontractor's area(s) of responsibility under the proposal C. The anticipated dollar amount for each subcontract D. Each subcontractor's form of organization E. An indication from each subcontractor of a willingness to carry out their responsibilities (this assurance in no way relieves the Respondent of any responsibilities in responding to this RFP or in completing the commitments documented in this proposal) F. The qualifications of each subcontractor for guaranteeing performance G. Identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience in the technical proposal for each portion of the proposed products or services to be provided by the subcontractor H. Any other data that may be required by the State	TCS intends to use GeoComm for its GIS services and Direct Technology for its ECaTS reporting software. Please see Section 4.3 [RFP 2.3.9] in business proposal for items A through H for each.

2.3.10 GENERAL INFORMATION

Business Information

	Enter your response below.
Legal Name of Company	**TeleCommunication Systems, Inc.**
Contact Name	**David Gleason**
Contact Title	**Regional Account Manager**
Contact E-mail Address	**david.gleason@comtechtel.com**
Company Mailing Address	**275 West Street**
Company City, State, Zip	**Annapolis, Maryland 21401**
Company Telephone Number	**410-263-7616**
Company Fax Number	**410-280-4903**
Company Website Address	**www.telecomsys.com**
Number of Employees (company)	**1,100**
Years of Experience	**28**
Number of U.S. Offices	**13**
Year Alabama Office Established (if applicable)	
Parent Company (if applicable)	**Comtech Telecommunications Corp.**
Revenues ($MM, prior year)	**TCS: $359.9M (2014)**

Revenues ($MM, two-years prior)	**TCS: $362.3M (2013)**
% Of Revenue from Alabama customers	

	Yes / No	**If No, Explanation**
Does your company have a formal disaster recovery plan? If no, please provide an explanation of any alternative solution your company has to offer. If yes, please note and include as an attachment.	**Yes**	

	Enter your response below. Please indicate if attachments are included.
What is your company's technology and process for securing any Board or private information that is maintained by your company?	The TCS Information Security Policy is established to protect the information assets of our organization, customers, and suppliers from all threats whether internal or external, deliberate or accidental, as well as to comply with all governing laws. The intent of this Policy is to outline the structure of our Information Security Management System (ISMS) and demonstrate compliance with the ISO 27001 Information Security standard. The ISMS will protect the information assets that reside within TCS, including information residing on the infrastructure and systems we use to conduct business. All TCS/Comtech information is maintained according to our Media Handling Procedure. The requirements within this procedure are mandatory and include asset classification, treatment levels, and associated handling requirements (such as encryption, direct delivery, or physical controls).

2.3.11 EXPERIENCE SERVING STATE GOVERNMENTS

	Enter your response below. Please indicate if attachments are included.
Please provide a brief description of your company's experience in serving state governments and/or quasi-governmental accounts. Disclose each state or jurisdiction in which Respondent does business or holds contracts to provide goods or services and the nature of each such business or contract.	TCS has provided statewide ESInet solutions of similar scope. We have listed specific information for these implementations in the references section above.

2.3.12 EXPERIENCE SERVING SIMILAR CLIENTS

	Enter your response below. Please indicate if attachments are included.
Please describe your company's experience in serving clients of a similar size to the State that also had a similar scope. Please provide specific clients and detailed examples.	TCS has provided statewide ESInet solutions of similar scope. We have listed specific information for these implementations in the references section above.

Alabama Next Generation 9-1-1 Systems and Services

AL-NG911-RFP-16-001

Technical Proposal

March 4, 2016

Submitted to:

Leah Missildine
Interim Executive Director
Alabama 9-1-1 Board
Reference: AL-NG911-RFP-16-001
1 Commerce Street
Suite 610
Montgomery, AL 36104
334.440.7911
leah@al911board.com

Prepared by:

TCS TeleCommunication Systems
Enabling Convergent Technologies®

David Gleason
Regional Account Manager
TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401
802.473.2005
david.gleason@comtechtel.com
www.telecomsys.com

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®, 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™, 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 439 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.

Table of Contents

Glossary vi

1. Technical Specifications [RFP Attachment D] 1

2. Cybersecurity Assessment Option 162

2.1. TCS Security Solutions: Let Us Help Protect the Assets You Can't Afford to Lose162

2.2. Comprehensive Security Assessment 162

2.3. External Network Security Assessment 164

2.4. Internal Vulnerability Assessment 166

2.5. Web Application Security Assessment 166

2.6. Wireless Network Survey 167

2.7. Security Awareness Service 167

2.7.1. Security Awareness Training 167

2.7.2. Social Engineering Assessment 168

2.7.3. Methodology and Approach for Social Engineering Testing 168

2.8. Reporting and Debrief 169

2.9. Protection of Information 170

2.10. Project Approach 170

2.10.1. Rules of Engagement 170

2.10.2. Project Timeline 171

2.11. Qualifications of Staff 171

2.12. About TCS 172

List of Exhibits

Exhibit 1. Network Diagram 20

Exhibit 2. Application Redundancy Diagram 21

Exhibit 3. ESInet Features and Functions 22

Exhibit 4. ALI DBMS Features 30

Exhibit 5. Network Specifications 32

Exhibit 6. Mean Opinion Score by Codec 32

Exhibit 7. Auxiliary Network Connections 33

Exhibit 8. TCS Security Architecture 46

Exhibit 9. Texting Solution Overview 52
Exhibit 10. EMedia Reporting Screenshot 53
Exhibit 11. ECaTS i3 Logger 54
Exhibit 12. ECaTS Connectivity to PSAP 54
Exhibit 13. Transfer Capability 56
Exhibit 14. TCS EMedia Solutions 57
Exhibit 15. Intrepid9-1-1 Solution Components 59
Exhibit 16. Topology Quality Control 68
Exhibit 17. Intrepid9-1-1 User Adds Time of Day Rule. 72
Exhibit 18. Intrepid9-1-1 Confirmation Screen 72
Exhibit 19. Intrepid9-1-1 Summary View of Transaction Logs 72
Exhibit 20. Call Flow Diagram 74
Exhibit 21. Location Validation Function 78
Exhibit 22. ALI DBMS Features 81
Exhibit 23. Table of Contents from TCS' Established Disaster Recovery Plan 83
Exhibit 24. ECaTS Interface 85
Exhibit 25. Sample ECaTS Reports 86
Exhibit 26. Call Transfer Count Report 88
Exhibit 27. ECaTS Graphical Capabilities 89
Exhibit 28. Wireless Call Sector Report 91
Exhibit 29. ECaTS User Login Screen 92
Exhibit 30. Password Management System 93
Exhibit 31. User Role Management Administration 94
Exhibit 32. Report Access Control System 95
Exhibit 33. PSAP Group Access Management 96
Exhibit 34. Schedule Report Interface 98
Exhibit 35. Raw CDR Viewer Interface 99
Exhibit 36. Raw CDR Collected from Viper 101
Exhibit 37. Raw CDR Collected from Sentinel/Vesta 101
Exhibit 38. Standard Reporting Output Options 102
Exhibit 39. System Health Interface 104
Exhibit 40. Ad Hoc Button on ECaTS Portal Screen 105

Exhibit 41. Ad-Hoc Homepage.......... 106
Exhibit 42. Standard Ad-Hoc Filters 106
Exhibit 43. Standard Ad-Hoc Interface 107
Exhibit 44. Information Button for Each Filter Field 108
Exhibit 45. Selecting Time Window for Report 108
Exhibit 46. Output Options 108
Exhibit 47. Filters.......... 109
Exhibit 48. Report Result (Excel Format) 109
Exhibit 49. Advanced Ad-Hoc Interface 110
Exhibit 50. Report Filters.......... 110
Exhibit 51. Report Results 111
Exhibit 52. Hanging State Dashboard Mockup 112
Exhibit 53. State Dashboard Overview.......... 113
Exhibit 54. Dashboard Widgets 113
Exhibit 55. Dashboard Widgets Description 113
Exhibit 56. Payload Processing Times.......... 116
Exhibit 57. Initial Station Total Calls Report Example 116
Exhibit 58. Ad-Hoc Report Example.......... 116
Exhibit 59. Answer Time Report Example.......... 117
Exhibit 60. Answer Seconds Field Available in Ad-Hoc Report 117
Exhibit 61. Disconnect Time 118
Exhibit 62. Ad-Hoc Report Example.......... 118
Exhibit 63. Total Count by Payloads Type 119
Exhibit 64. Average Event Waiting Report 119
Exhibit 65. Average Event Duration Ad-Hoc Report.......... 120
Exhibit 66. Event Summary Report 120
Exhibit 67. Abandoned Events Per Hour 120
Exhibit 68. Events by Incoming IP Address 121
Exhibit 69. Events Per Hour Report Example 121
Exhibit 70. Initial Station Total Events Report Example 122
Exhibit 71. Ad-Hoc Report Example.......... 122
Exhibit 72. Events by Operator Report Example.......... 122

Exhibit 73. Operator Speed of Answer Report Example 123
Exhibit 74. Ad-Hoc Report Example 123
Exhibit 75. Events per Hour by Day of Week Report Example 124
Exhibit 76. Report Interface with Drop-Down Menus 125
Exhibit 77. Calls with Multiple Transfers Appearing as Chain 125
Exhibit 78. Ad-Hoc Report Showing Transferred Calls 126
Exhibit 79. Report Parameters Example 126
Exhibit 80. Agent Availability Report Example 126
Exhibit 81. Event Summary Report 127
Exhibit 82. Individual Call Detail 127
Exhibit 83. Individual Call Detail Report Example 128
Exhibit 84. Individual Call Detail Report Example 128
Exhibit 85. Utilization Report Example 129
Exhibit 86. Time of Payload Entry Through BCF Report 131
Exhibit 87. End-to-End Routing Report 131
Exhibit 88. Answer Time Report Example 132
Exhibit 89. Maintenance/Configuration Events with Date/Time Ranges 133
Exhibit 90. PSAP Outage Notification Showing ALI Format Issue Details 133
Exhibit 91. SIL Table 138
Exhibit 92. TCS Network Operations Center 142
Exhibit 93. Sample MNS Report 145
Exhibit 94. Event Analysis Screenshot 147
Exhibit 95. Network Performance – Interface Data Example 148
Exhibit 96. Intrepid9-1-1 ESInet Implementation Schedule 155
Exhibit 97. CLC Test Plan Table of Contents 1 of 2 157
Exhibit 98. CLC Test Plan Table of Contents 2 of 2 158
Exhibit 99. PSAP Test Plan Table of Contents 159
Exhibit 100. Transition Plan Table of Contents 160
Exhibit 101. Typical PSAP Connectivity 163
Exhibit 102. ESInet Connectivity 164
Exhibit 103. TCS Network Penetration Testing Methodology 165
Exhibit 104. Program Organization Chart 172

Glossary

Term	Definition
ACL	Access List
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
AL9-1-1	Alabama 9-1-1 Board
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AP	Access Point
AQPS	ALI Quality Process Services
ASA	Alabama Supercomputer Authority
ATIS	Alliance for Telecommunications Industry Solutions
B2BUA	Back-to-Back User Agent
BCF	Border Control Function
BGP	Border Gateway Protocol
CAD	Computer-Aided Dispatch
CAMA	Centralized Automatic Message Accounting
CBWFQ	Class Based Weighted Fair Queuing
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
CoS	Class of Service
COTS	Commercial Off-the-Shelf
CPE	Customer Premise Equipment

Term	Definition
CSA	Canadian Standards Association
CSP	Communications Service Provider
CSRIC	Communications Security, Reliability and Interoperability Council
CVSS	Common Vulnerability Scoring System
DACS	Digital Access and Cross-Connect System
DBMS	Database Management System
DNS	Domain Name Server
DoD	Department of Defense
DoS	Denial of Service
DSCP	Differentiated Services Code Point
E9-1-1	Enhanced 9-1-1
ECaTS	Emergency Call Tracking System
ECD	Emergency Communications District
ECRF	Emergency Call Routing Function
EIA	Electronic Industries Alliance
E-MF	Enhanced Multifrequency
EMI	Electromagnetic Interference
ESA	Emergency Service Agency
ESGW	Emergency Services Gateway
ESIND	Emergency Services IP Network Design
ESInet	Emergency Services IP Network
ESP	Enterprise Security and Protection
ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Proxy
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
GIS	Geographic Information System
GMLC	Gateway Mobile Location Center

Term	Definition
GUI	Graphical User Interface
HELD	HTTP-Enabled Location Delivery
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBOP	Implementation and Back-Out Plan
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IPS	Intrusion Prevention System
ISDN	Integrated Services Digital Network
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISUP	ISDN User Part
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LbyR	Location by Reference
LbyV	Location by Value
LEC	Local Exchange Carrier
LIF	Location Interwork Function
LIS	Location Information Server
LMR	Land Mobile Radio
LNG	Legacy Network Gateway
LoST	Location to Service Translation
LPG	Legacy PSAP Gateway
LSRG	Legacy Selective Router Gateway

Term	Definition
LTE	Long Term Evolution
LVF	Location Validation Function
MDN	Mobile Directory Number
MF	Multifrequency
MIS	Management Information System
MLP	Mobile Location Protocol
MNS	Managed Network Services
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
NEMA	National Electrical Manufacturers Association
NENA	National Emergency Number Association
NG	Next Generation
NG9-1-1	Next Generation 9-1-1
NGCS	Next Generation Core Services
NG-SEC	NENA 75-001 Security for Next Generation 9-1-1 Standard
NIF	NG9-1-1–Specific Interwork Function
NMS	Network Management System
NOC	Network Operations Center
NTP	Network Time Protocol
NxGnCo	NextGen Communications, Inc.
OGC	Open Geospatial Consortium
OS	Operating System
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
P2P	Peer to Peer

Term	Definition
PAM	PSAP-to-ALI Message
pANI	Pseudo Automatic Number Identification
PBX	Private Branch Exchange
PDU	Power Distribution Unit
PIDF-LO	Presence Information Data Format – Location Object
PIF	Protocol Interwork Function
PMO	Program Management Office
PNL	Preferred Network List
POI	Point of Ingress/Interconnection
POTS	Plain Old Telephone Service
PRF	Policy Routing Function
PRI	Primary Rate Interface
PS/ALI	Private Switch Automatic Location Identification
PSAP	Public Safety Answering Point
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QC	Quality Control
QoS	Quality of Service
RCA	Root Cause Analysis
RFAI	Request for Additional Information
RFC	Request for Comment
RFP	Request for Proposal
RTP	Real-Time Transfer Protocol
SBC	Session Border Controller
SDE	Spatial Database Engine
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIF	Spatial Information Function
SIL	Service Impact Level
SIP	Session Initiation Protocol

Term	Definition
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOI	Service Order Input
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SQL	Structured Query Language
SR	Selective Router
SS7	Signaling System 7
TCC	Text Control Center
TCP	Transmission Control Protocol
TCS	TeleCommunication Systems, Inc.
TDM	Time-Division Multiplexing
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TTY	Teletypewriter
TVSS	Transient Voltage Surge Suppression
UL	Underwriters Laboratories
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UTC	Coordinated Universal Time
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WFS	Web Feature Service
WGS	World Geodetic System
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
XML	Extensible Markup Language

1. Technical Specifications [RFP Attachment D]

SECTION 1 RESPONSE INSTRUCTIONS

1.1 GENERAL RESPONSE INSTRUCTIONS

Respondents must respond with either COMPLY, NON COMPLY or EXCEPTION to all of the sections and requirements in this RFP.

It is recommended that all detailed responses are located under the section heading and section verbiage to aid in evaluation. Enter your response(s) in line with the sections and requirements at the end of each section. If no clear order is followed; the response may be disqualified.

Respondents that take an EXCEPTION to a particular requirement must provide an alternative to the required feature or function specified. The alternative must describe in detail how it meets the original requirement and must include any other pertinent information that may be necessary to properly consider the alternative being offered (i.e. diagrams, enhanced capability, design efficiency, cost savings, etc.).

The Board recognizes that in some cases Respondents may be able to provide a service or function that is superior to the requirements listed. If the Respondent wishes to present such an alternative, an EXCEPTION should be used to clearly articulate the functionality that Respondents would like to propose as an alternative for evaluation.

The requirements specified in this RFP are identified as MUST haves, SHALL haves, REQUIRED, REQUIRES, or REQUIREMENT(S).

Each proposal will be evaluated according to how well the requirements have been addressed.

Features and functions listed as DESIRABLE are not required. Desirable features and functions add value to a requirement. Respondents are encouraged to provide desirable features and functions where they have an opportunity to maximize the value to the Board while also satisfying the underlying requirement.

Desirable features, functions or elements are described in the RFP as SHOULD, MAY, COULD or DESIRED.

1.2 SCOPE OF PROCUREMENT

1.2.1 PURPOSE

The Alabama 9-1-1 Board (AL9-1-1, the Board) seeks competitive bids from qualified vendors to provide integrated network services for the operation of the ANGEN Network currently serving the PSAPs of Alabama. Alabama is currently served by a wireless 9-1-1 call delivery network known as ANGEN.

The purpose of this procurement is to ensure that at a minimum, the current services provided by the existing ANGEN Network are continued and improved upon as technology, standards, and societal demands evolve.

The AL9-1-1 Board invites qualified vendors with documented expertise and experience to submit proposals to provide wireless and wireline E9-1-1 call delivery, i3 ESInet Network Services, reporting, monitoring, service and support for the operation of the ANGEN Network.

TCS Response: Comply.

TCS is a qualified vendor that can leverage the use of Alabama's current ANGEN network and data facilities in Montgomery and Huntsville to provide wireless and wireline E9-1-1 call delivery, i3-compliant ESInet network services, reporting and monitoring, plus service and support for the operation of the ANGEN network.

1.2.2 PROJECT OVERVIEW

This procurement will result in the selection of a service provider or a combination of service providers whose proposed solution(s) and services as sought by this RFP will at a minimum, provide the existing level of service as provided by the current ANGEN network to include all existing capabilities, functions, components and ancillary services to all Alabama PSAPs either directly or in collaboration with other systems, services and providers both in Alabama and in adjoining states (MS, TN, FL and GA).

This RFP does not include PSAP CPE, PSAP call taking equipment, furniture, computers or other operational systems required by PSAPs. It is focused only on the services required for the operation of the ANGEN Network and the services it provides to Alabama PSAPs.

The solution(s) and services sought through this RFP may be proposed as an integrated, comprehensive solution, or as a stand-alone component representing a best in class service offering capable of being integrated with other components that will comprise the ANGEN ecosystem.

The Board may, at its discretion, integrate proposed solutions or components of proposed solutions in order to achieve an enterprise-wide, statewide, best in class system that benefits all Alabama PSAPs and best serves the Board in fulfilling its duties under the law.

The Board would prefer an integrated solution with a designated primary vendor contractually responsible for providing the services as specified in this RFP.

The Board may, at its discretion, designate a contractual prime vendor and require contractual relationships, cooperative agreements, interconnection to and interaction with other system service providers or third parties as required or necessary for the operation of ANGEN.

Through this procurement the Board seeks to procure a solution or combination of solutions that:

1. Are designed to industry standard including the NENA i3 standard (Section 1.6)

2. Provides or supports a foundation for NG9-1-1 and is designed to support or interoperate with core i3 functionality (Section 4)

3. Are secure and resilient to cyber-attack, penetration, abuse or misuse (Section 2)

4. Provide the ability to alarm, report, monitor, manage and support on a 24/7/365 basis (Section 6)

5. Be able to support or integrate with Interim SMS Text-to-9-1-1 solutions that are currently in-place or planned via delivery methods as prescribed by the Board, as per FCC order or by Carrier consent decree (Section 3)

a. Both inbound and outbound via a TCC and/or through the use of direct SIP based MSRP messaging as prescribed in NENA i3

6. Provides or Supports Wireless and Wireline E9-1-1 Call Routing and Data Delivery (Section 3)

a. Is capable of the primary receipt, routing and delivery of Wireless 9-1-1 calls from wireless carriers via an ESInet to any PSAP throughout Alabama and neighboring states (MS, TN, GA, FL) or

b. A solution capable of supporting, integrating with and assisting in the delivery of Wireline E9-1-1 Calls to any Alabama PSAP and neighboring states.

c. A solution capable of supporting, integrating with and assisting in the delivery of Wireless E9-1-1 Calls to any Alabama PSAP and neighboring states.

7. Provides or supports Increased fault tolerance, reliability, resiliency and disaster recovery across Alabama (Section 2)

8. Provides for or supports Enterprise wide call accounting and data collection (Section 5)

TCS Response: Comply.

TCS understands the project overview and can meet the above-listed requirements.

1.2.3 SCOPE OF SERVICES

The Board is seeking to procure services from qualified vendors that include the highest degree of resiliency, reliability and redundancy to ensure service availability in keeping with industry standard and best practices.

The services sought by this RFP include:

1. ESInet network design, management, and operation services

2. NG, i3 core functions and capabilities

3. Wireless and Wireline E9-1-1 call routing and reporting services

4. Text to 9-1-1 services

5. Enterprise/State-wide data collection and reporting services on all ANGEN facilitated transactions

6. System and component level monitoring, alarming, diagnostics and reporting services

7. Disaster recovery and system restoration services

8. 24/7/365 Help desk, trouble ticketing and customer facing support services

9. 24/7/365 Network operations center (NOC) monitoring services

10. Installation, testing, maintenance and on-site support services

11. Project management services for the planning, design, testing, installation and operation of the system or systems

TCS Response: Comply.

TCS understands the scope of services and can meet the above-listed requirements.

The Board does not favor one technology or platform. This RFP is designed to allow providers to package, represent and demonstrate their services. The Board will evaluate each service on its own merit to determine the best solution(s) for the State of Alabama.

This overview of the Scope of the effort is meant to provide a high level understanding of the objectives. This technical specification provides greater detail of the requirements in the following sections.

TCS Response: Comply.

TCS understands the scope of this project.

1.3 STANDARDS

Respondents shall demonstrate their industry knowledge and describe their commitment to providing standards based solutions and services.

The Board may disqualify or reject non-standard or proprietary systems that may hinder NG9-1-1 implementation, limit interoperability, or that might restrict the State from interconnecting to a regional or national 9-1-1 system in the future.

Throughout the duration of the project, Respondents shall maintain compliance with all standards and ensure that the products, solutions and services provided for ANGEN evolve and adapt as the standards evolve.

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

- NENA 08-003 v1 Detailed Functional and Interface Specification for the NENA i3 Solution, Stage 3 Version 1
- NENA 08-002 NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3)
- NENA 08-751 NENA i3 Technical Requirements Document
- NENA 04-001 v2 PSAP E9-1-1 PSAP Equipment
- NENA 58-001 NENA IP-Capable PSAP Minimum Operational Requirements Standards
- NENA 58-501 IP PSAP 9-1-1 System Features and Capabilities
- NENA 75-001 Security for Next Generation 9-1-1 Standard (NG-SEC), NENA 75-001 v1, and NENA 04-503 v1
- NENA 75-502, NENA 04-502 v1, NENA 04-503 v1, NENA 08-506 v1, NENA 08-752 v1, NENA 71-502 v1, NENA STA-003
- Applicable Internet Engineering Task Force Standards (IETF), such as IP protocols, IP routing protocols, SIP, RTP, LoST, and the PIDF-LO
- NENA 08-506 Emergency Services IP Network Design for NG9-1-1

While specific standards and documents are referenced in the list above, the Board acknowledges that work on these standards is underway and that many of these standards are in the process of being updated and at the time of RFP distribution may now be referenced by a different number or nomenclature. If there are any discrepancies between the items listed above and a current standard or informational document, the most current version will apply.

Respondents shall describe in detail in the response how they shall meet such standards in their design.

TCS Response: Comply.

TCS complies with the above-listed NENA standards.

NENA Compliance

Intrepid9-1-1 fully complies with the NENA i3 standard for foundation-level NG-9-1-1 systems and architecture. TCS personnel are involved in creating, implementing, and improving current and future NENA standards, to which the Intrepid9-1-1 is aligned.

We developed our solution from the ground up to comply with National Emergency Number Association (NENA) standards – specifically, the NENA i3 standard – because they provide the best path for deploying a system that leverages current technology while enabling customers to maintain an optimal system. Aside from the clear transition in technology – moving from Time-Division Multiplexing (TDM) to Internet Protocol (IP) – one of the most important aspects of an NG9-1-1 system is its ability to route calls based on the caller's actual location. In 1999, TCS created a patented solution for spatial routing of 9-1-1 calls. Today, we use our technology to deliver NG9-1-1 calls with our NENA i3-compliant network solutions.

Our Intrepid9-1-1 NGCS product line features advanced capabilities combined with performance, scalability, and availability. Intrepid9-1-1's enterprise-grade components comply with the NENA i3 standard, while affording modular and cost-effective configurations to public safety agencies of all sizes.

Involvement with Standards Development

TCS has been a primary author of the National Emergency Number Association (NENA) NG9-1-1 vision, requirements, architecture, and standards. This includes the NENA i3 STA 010 (prev. 08-003) standard and other supporting best practices, informational documents, and specifications. TCS staff members continue to serve as part of NENA's Development Steering Council and dozens of active working groups across several of the NENA committees.

TCS is an active member of APCO, with ongoing involvement in the development of APCO best practices, informational guidelines, and American National Standards Institute (ANSI) developed industry standards.

TCS has been an active member of the FCC-sponsored Network Reliability & Interoperability Council (NRIC), the series culminating with NRIC VII running from January 6, 2004 through January 6, 2006, and has been active in the subsequent current series known as Communications Security, Reliability and Interoperability Council's (CSRIC). Maurice Tosé, TCS' chairman and Chief Executive Officer, is currently a member of CSRIC V, chartered from March 18, 2015 through March 18, 2017.

The TCS solution fully complies with the NENA i3 standard for foundation-level NG-9-1-1 systems and architecture and was built from the ground up to comply with NENA i3.

Federal Communications Commission Rules

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

Other Industry Standards

Where applicable, all equipment proposed to support or operate ANGEN must comply with applicable industry standards, such as:

- Underwriters Laboratories (UL)
- International Organization of Standards (ISO)
- Open System Interconnection (OSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)
- Electronic Industries Alliance (EIA)
- Telecommunications Industry Association (TIA), (including ANSI/EIA/TIA-568 Commercial Building Telecommunications Wiring Standards), etc.

TCS Response: Comply.

TCS complies with the above-listed standards.

1.3.1 OPEN STANDARDS

Respondents shall propose a system that utilizes an Open Standards methodology.

The proposed system shall be subject to standards that enhance open standards and increase interoperability such as ITU, IEEE 802 at ISO Layer-2, and IP and TCP, as defined by the IETF in the applicable RFCs, at ISO Layer-3 and above.

If proprietary standards or protocols are used within a proposed solution; Respondents shall disclose the proprietary nature and discuss any limitations that may result.

TCS Response: Comply.

TCS uses an open standards methodology.

1.4 ANGEN BACKGROUND

The state of Alabama has a long history of leadership in 9-1-1 services, claiming the nation’s first 9-1-1 call in 1968 over a local system in the town of Haleyville soon after AT&T announced the designation of 9-1-1 as a national emergency number.

More than 40 years later, the state’s circuit-switched copper-wire system was struggling to keep up with telecom advances that included wireless mobile phones and Voice over IP.

Work on the present day ANGEN system began in June 2012. Wireless traffic is the current primary focus of the ANGEN system because it accounts for the majority of emergency calls in Alabama, as much as 70 percent in some places.

The ultimate goal of ANGEN is to provide NG9-1-1 services that combine voice, video, text and data on a single emergency communications platform, to let callers use the services they are accustomed to on their smart phones and other devices when making emergency calls, as well as provide additional information to first responders.

ANGEN relies upon and uses the Alabama Supercomputer Authority backbone network (ASA) for interconnection between two aggregation points located in Huntsville AL and Montgomery AL.

All wireless carriers providing service in AL interconnect and aggregate all circuits used for wireless 9-1-1 traffic redundantly to these two aggregation points. This forms the basis for the current level of service for ANGEN.

Current ANGEN Partners include:

Local 9-1-1 Districts – All counties and some cities have 9-1-1 Districts to set policy and manage the local PSAP or PSAPs. County Commissions or City Councils appoint the District Boards, or the elected officials sometimes serve as the 9-1-1 Board.

Alabama 9-1-1 Board – The board is charged with administering the $1.75 collected monthly from each phone account for 9-1-1 expenses. The Alabama 9-1-1 Board administered the grant awarded to the Alabama Department of Homeland Security, which partially funded the implementation of ANGEN.

Bandwidth Inc – current system service provider provides the hardware, software, and support services to route wireless 9-1-1 calls to the proper PSAP using the legacy Selective Routers. There are two core facilities in different parts of the state, either of which can handle the entire State if needed.

Alabama Supercomputer Authority (ASA) – Provisions and manages the physical IP network and the redundant and diverse back-bone network that connects the two core facilities in Huntsville and Montgomery.

Current ANGEN Network Diagram

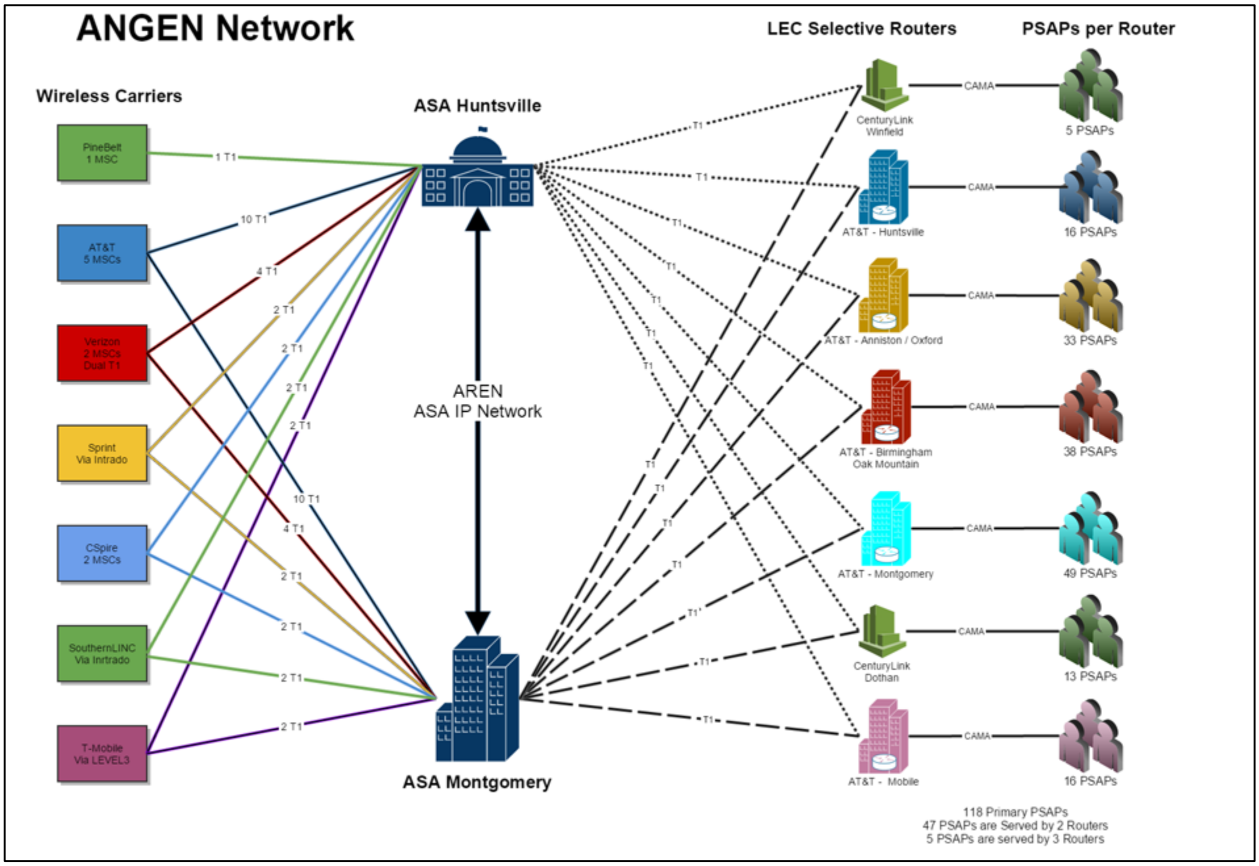
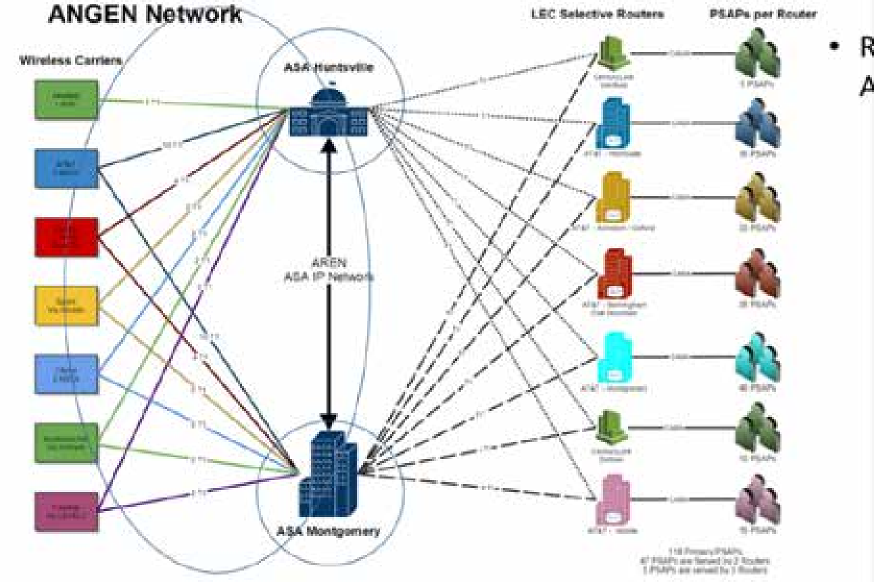


Figure 1 - Current ANGEN Connectivity Diagram

The diagram above represents the logical network connectivity currently employed by the ANGEN system. This diagram is current as of the distribution of this RFP. This diagram will be used and referenced here for the purposes of defining certain requirements and design considerations for any proposed solutions offered by Respondents.



- Require the use of existing ANGEN elements
  - Data centers in Huntsville and Montgomery
  - Terminating circuits, both ingress and egress

Figure 2 – Current ANGEN Component Re-Use Diagram

The Board's preference is to reuse and repurpose the existing elements of ANGEN represented in the diagram above. Respondents must take this into consideration in any solution proposed and designed in response to this RFP.

Due to the critical nature of operational specifics regarding the capabilities and operation of ANGEN, additional details and information related to the current ANGEN design, configuration, capabilities, connections and operations will be shared with Respondents deemed qualified after the initial receipt of proposals to this RFP.

ANGEN 2015 Operating Metrics

2015 ANGEN Call Volumes By County

County	2015 Total	Average Month	% State
Jefferson	571,830	47,653	20.9077%
Mobile	284,576	23,715	10.4049%
Montgomery	210,670	17,556	7.7027%
Madison	152,949	12,746	5.5922%
Tuscaloosa	138,640	11,553	5.0691%
Baldwin	77,515	6,460	2.8342%
Lee	70,111	5,843	2.5634%
Shelby	61,533	5,128	2.2498%

Houston	56,803	4,734	2.0769%
Etowah	55,720	4,643	2.0373%
Calhoun	51,523	4,294	1.8838%
Russell	48,684	4,057	1.7800%
Morgan	46,305	3,859	1.6930%
Talladega	45,321	3,777	1.6571%
Lauderdale	41,298	3,442	1.5100%
Dallas	41,044	3,420	1.5007%
Cullman	34,702	2,892	1.2688%
Marshall	33,925	2,827	1.2404%
St Clair	33,867	2,822	1.2383%
Elmore	32,522	2,710	1.1891%
Walker	31,516	2,626	1.1523%
Limestone	25,180	2,098	0.9206%
Colbert	24,895	2,075	0.9102%
Escambia	24,571	2,048	0.8984%
Chilton	23,117	1,926	0.8452%
Blount	22,896	1,908	0.8371%
Autauga	21,362	1,780	0.7811%
Coffee	21,178	1,765	0.7743%
Dale	20,105	1,675	0.7351%
Butler	19,534	1,628	0.7142%
DeKalb	19,174	1,598	0.7011%
Chambers	18,931	1,578	0.6922%

Marion	17,552	1,463	0.6417%
Covington	16,703	1,392	0.6107%
Marengo	16,251	1,354	0.5942%
Pike	15,907	1,326	0.5816%
Tallapoosa	15,805	1,317	0.5779%
Franklin	15,769	1,314	0.5766%
Macon	15,523	1,294	0.5676%
Sumter	15,033	1,253	0.5496%
Pickens	14,943	1,245	0.5464%
Jackson	14,942	1,245	0.5463%
Monroe	13,168	1,097	0.4815%
Lawrence	12,819	1,068	0.4687%
Greene	12,689	1,057	0.4639%
Clarke	12,583	1,049	0.4601%
Hale	11,516	960	0.4211%
Barbour	11,360	947	0.4154%
Geneva	10,746	896	0.3929%
Cherokee	10,580	882	0.3868%
Lowndes	10,263	855	0.3752%
Perry	10,199	850	0.3729%
Winston	10,084	840	0.3687%
Conecuh	9,252	771	0.3383%
Bibb	8,457	705	0.3092%
Cleburne	7,841	653	0.2867%

Wilcox	7,615	635	0.2784%
Washington	7,603	634	0.2780%
Lamar	6,787	566	0.2482%
Crenshaw	6,629	552	0.2424%
Randolph	6,609	551	0.2416%
Choctaw	6,242	520	0.2282%
Fayette	5,648	471	0.2065%
Henry	4,910	409	0.1795%
Bullock	4,475	373	0.1636%
Clay	3,353	279	0.1226%
Coosa	3,174	265	0.1161%
Grand Total	2,735,027	227,919	100.0000%

Table 1 - 2015 ANGEN Call Volumes by County

The table above represents the ANGEN operational call volumes by AL county for 2015. These figures represent all Wireless E9-1-1 calls processed in Alabama in 2015 and processed by the ANGEN system. This table can be used for reference in design considerations of any proposed solutions provided in response to this RFP.

Current ANGEN Call Volumes by Month 2015

The chart below depicts actual wireless E9-1-1 call volumes by month of the ANGEN system. The information represented below can be used for estimating system capacities and call volumes and can be used as a basis for developing initial cost estimates.

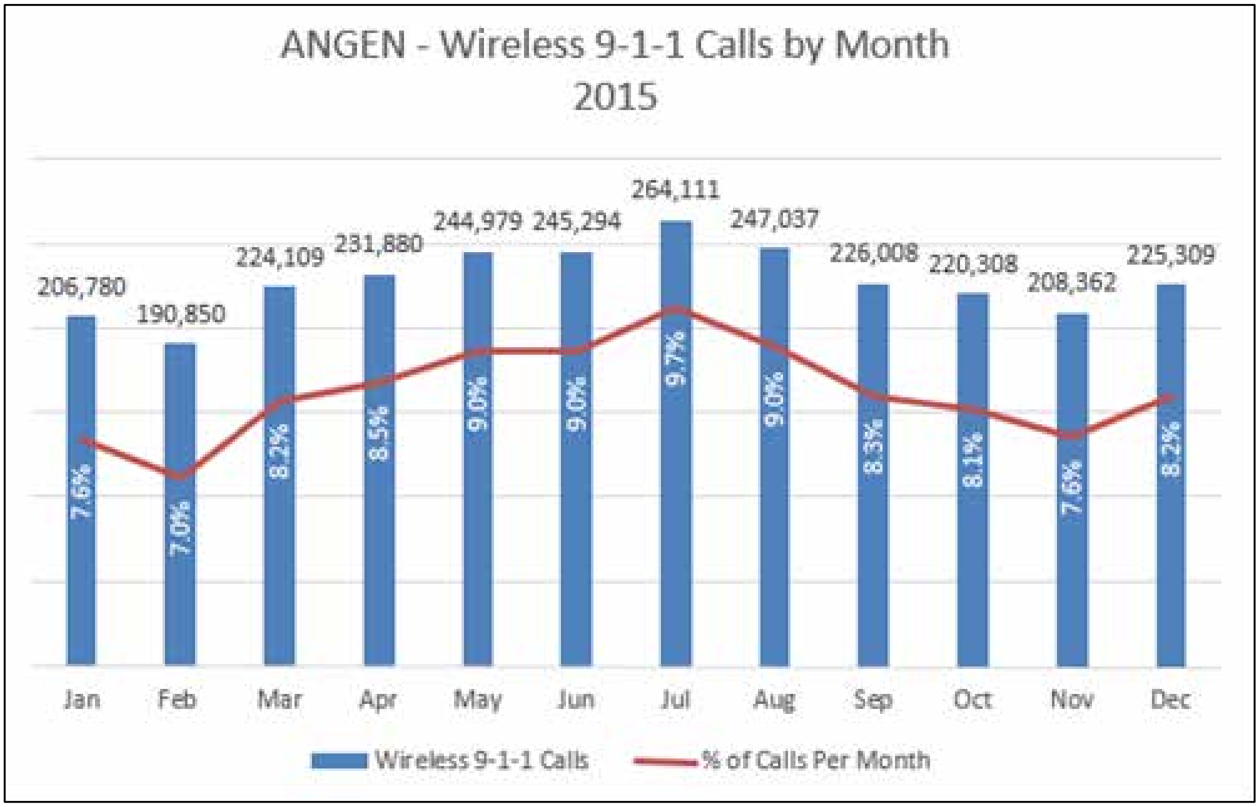


Figure 3 - Chart of ANGEN Call Volumes by Month 2015

Current ANGEN Call Routing Diagram

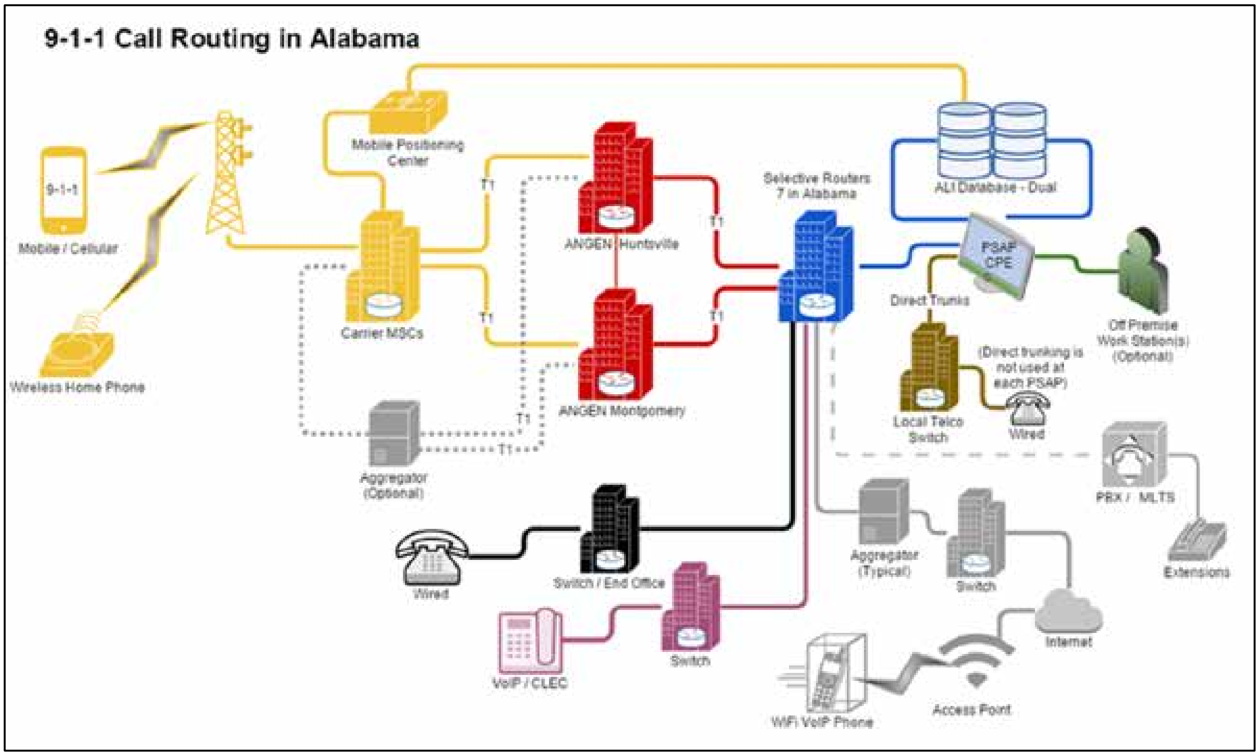


Figure 4 – Current ANGEN Call Routing Diagram

The diagram above provides the logical call flow and routing of the current ANGEN system. Additional details include:

- Each carrier purchases the network to the core facilities and the State's vendor purchases the circuits to the selective routers.
- Emergency Communications Districts (ECDs) purchase the circuits from the selective routers to the PSAP.

SECTION 2 ANGEN ESINET REQUIREMENTS

This section provides the ANGEN ESInet requirements and design considerations for Respondent’s to this RFP.

2.1 ANGEN ESINET DESIGN GOALS AND OBJECTIVES

ANGEN Conceptual Design Diagrams for Reference

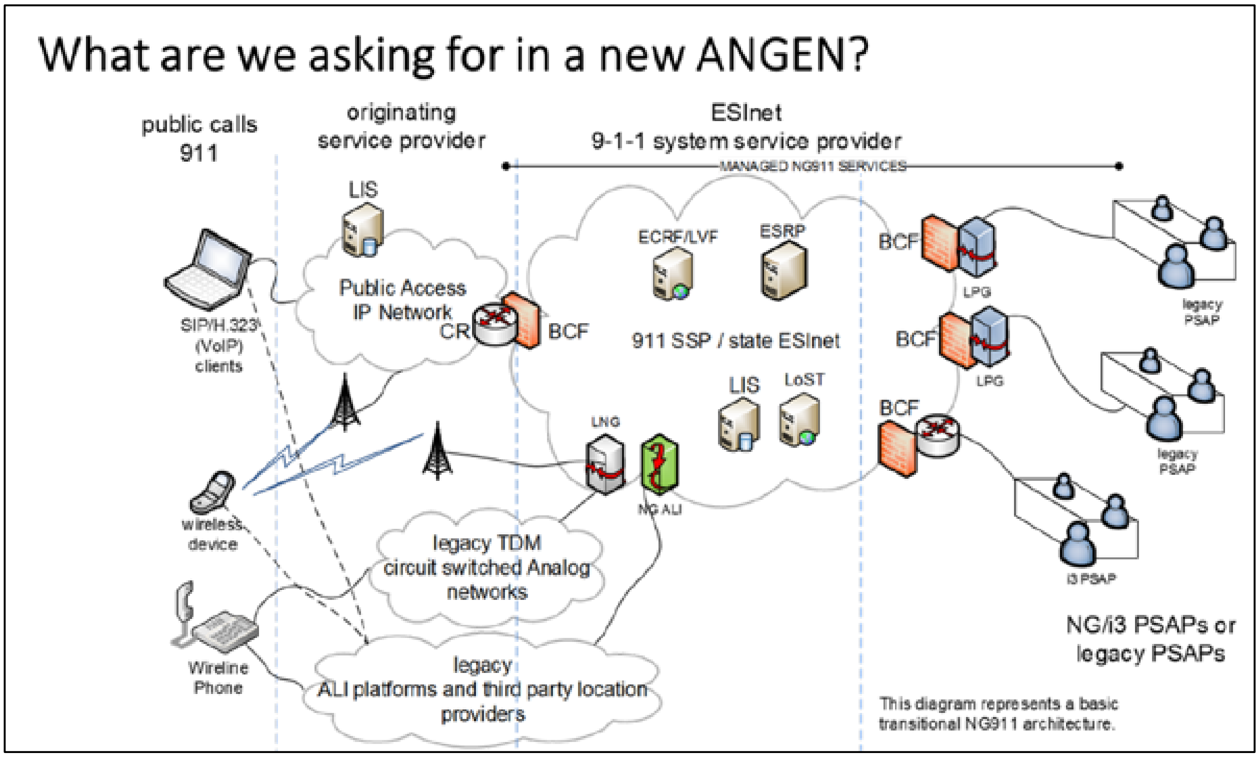
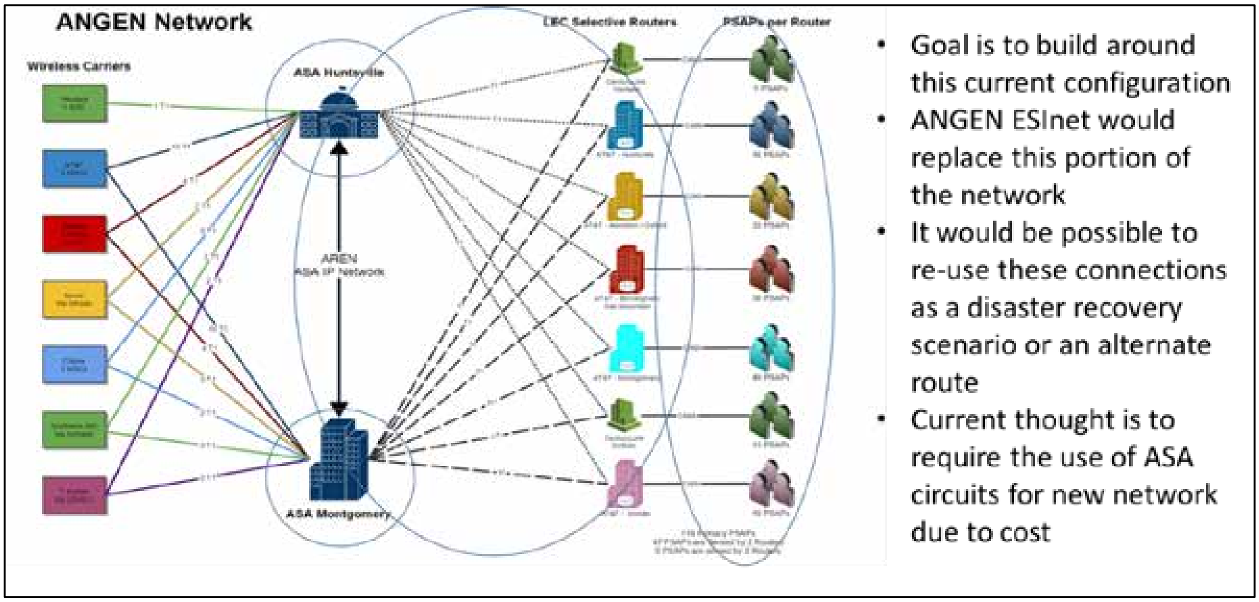

What are we asking for in a new ANGEN?
public calls 911
originating service provider
ESInet 9-1-1 system service provider
MANAGED NG911 SERVICES
LIS
Public Access IP Network
CR
BCF
SIP/H.323 (VoIP) clients
ECRF/LVF
ESRP
911 SSP / state ESInet
LIS
LoST
LNG
NG ALI
BCF
LPG
BCF
LPG
BCF
legacy PSAP
legacy PSAP
i3 PSAP
wireless device
legacy TDM circuit switched Analog networks
Wireline Phone
legacy ALI platforms and third party location providers
NG/i3 PSAPs or legacy PSAPs
This diagram represents a basic transitional NG911 architecture.

Figure 5 - ANGEN Conceptual Design Diagram

The diagram above represents the conceptual end state of the Future ANGEN system and services as desired by the Board and sought by this RFP. The ESInet will be designed to support and facilitate the operational services provided by the ANGEN system functional elements represented in the diagram above.

TCS Response: Comply.

TCS’ proposed design is based on the above description of Alabama’s statewide ESInet.



- Goal is to build around this current configuration
- ANGEN ESInet would replace this portion of the network
- It would be possible to re-use these connections as a disaster recovery scenario or an alternate route
- Current thought is to require the use of ASA circuits for new network due to cost

Figure 6 - ANGEN ESInet Goals and Design Considerations

PSAP Information

Alabama is made up of 67 counties with a population of 4,850,000. This population is served by 88 Emergency Communications Districts representing 118 Primary PSAPs. For the purposes of this procurement, the following number of PSAPs are within the scope of this project and anticipated services.

1. There are 118 Primary PSAPs in the state.
2. There are 88 ECDs in the state

For the purposes of this procurement, any solutions or services that require provisioning to a PSAP, the number of PSAPs to be considered will be 118 as explained and derived above.

All of the 118 PSAPs are currently operational and fully deployed E9-1-1, Wireless Phase 1 and Phase 2.

Specific address information for each of the 118 Alabama PSAPs covered by this RFP will be made available to qualified respondents as appropriate and necessary for the refinement of costs and designs of proposed solution(s).

TCS Response: Comply.

TCS' design is based upon the above-listed metrics. Specific address information is necessary for us to have included actual network costs in this response. In the absence of specific addresses, we have provided rough-order-of-magnitude network pricing as a placeholder for actual firm fixed pricing.

2.2 ANGEN ESINET SERVICES

The Board seeks network and operations services from a provider or a combination of providers to implement an Emergency Services IP-network (ESInet) to deliver or support the delivery of voice, text, or other emergency communications related data to the PSAP's throughout Alabama and in the adjoining states of MS, TN, GA and FL or as may be designated by the Board.

The ESInet(s) will be the foundational technology for keeping Alabama on the forefront of the transition to Next Generation 9-1-1 features, functions and capabilities during the term of the contract and will form the core technology of the ANGEN ecosystem.

Respondents interested in providing ESInet services must design and provide an IP based network solution with the ability to connect and interconnect to other regional, state and potentially national emergency services networks (i.e. FirstNet).

The proposed solution must at a minimum deliver the same functionality of the current ANGEN system as detailed in Section 1 of this specification.

Successful respondents will provide all services necessary for the development, implementation operation, monitoring and maintenance of their proposed ESInet including:

- Design, installation, testing, interconnection and operation of ESInet components required to operate or support the operation of ANGEN
- Maintenance and repair of those elements of the ESInet and interconnections owned, operated, installed or controlled by Respondents as part of their solution
- Completion of as built drawings, sketches and/or schematic materials related to the ESInet
- A data collection and reporting system for all ESInet elements so operational metrics of the ESInet can be monitored, reported and analyzed

TCS Response: Comply.

TCS proposes a managed service approach for the ESInet and functional elements. All services necessary to deploy, implement, operate, monitor, and maintain the network are included in our pricing. We have proposes a tiered model of optional services that allow the state a great degree of flexibility as to how the network and services will be deployed.

As-built drawings and associated information will be provided after contract award and subsequent engineering discussions.

Similarly, a collection and reporting system will be discussed post-award to ensure operational metrics are understood and accounted for. Our systems provide a great deal of data collection and reporting capabilities that will allow the entire service to be appropriately monitored.

2.3 ANGEN ESINET ARCHITECTURE REQUIREMENTS

Any ESInet proposed in response to this RFP must conform to NENA 08-506, Emergency Services IP Network Design for NG9-1-1 (ESIND) and other industry standards as referenced in Section 1 of this specification.

ESInet design requirements include but are not limited to:

- The ESInet shall be designed with as few single points of failure as practical. Diverse network elements and paths, redundant equipment, and other technical and physical means will be used to reduce the potential for total loss of service where a single point of failure is not reasonably avoidable.
- The ESInet shall be designed with a minimum level of bandwidth to support delivery of calls and associated data from originating service providers or other integrated ESInets to the PSAPs.
- The ESInet shall be designed and deployed using a highly reliable and redundant architecture.
- Availability, diversity, redundancy and resiliency shall be the guiding ESInet design principals
- The ESInet design shall support the ability to automatically reroute traffic to alternate routes or systems in order to bypass network outages and system failures.
- The ESInet design shall offer the ability to prioritize critical traffic at multiple levels by importance of applications or users
- The ESInet design shall be scalable and have the ability to scale without adverse effects on performance or costs
- The ESInet shall be designed to support a guaranteed Quality of Service (QoS) level
- The ESInet shall be designed to support the automatic adjustment of traffic priorities in order to meet established QoS levels as defined in NENA 08-003
- The ESInet design shall support the ability to ensure performance through the use of traffic shaping and traffic policing.
- The ESInet shall be designed to operate on a 24x7x365 basis.
- An ESInet design that utilizes the most cost effective and feasible combination of transport technologies available to deliver the bandwidth required.
- The ESInet design shall support the ability to handle legacy 9-1-1 calls and ensure the capability of handling future call types.

TCS Response: Comply.

TCS complies with the requirements above. We design our systems for active–active call processing with both local and geo-redundant applications so there are no single points of failure in the service. Likewise, where practical, we design our network with diverse carriers to ensure no single point of failure, although not all sites allow for this diversity. Combined, our service is designed for 99.999% availability and operated and maintained 24x7.

We also design the system to support 100% of the traffic from a single site, which takes into account both the bandwidth and the systems necessary to provide full redundancy. The network itself is a highly available network mesh (assuming a public safety-grade network is selected) such as an MPLS network. An MPLS network is designed to reroute traffic as needed to reach the desired endpoint, and our applications are built to do the same. Quality of Service (QoS) traffic marking will be used so that network traffic priority is respected to ensure voice and signaling paths are honored as the highest priority.

All critical applications offer the ability to be scaled as needed, with no “fork-lift” upgrades required. Similarly, the ESInet will be built to handle legacy 9-1-1 traffic at first, then scale its necessary applications to ensure that NG9-1-1 traffic (IP-based ingress) will be fully supported.

2.3.1 ESINET NETWORK DIAGRAM(S)

Respondents shall provide Network Diagrams to support their narrative that accurately displays how their proposed ESInet will be configured and deployed.

The Network Diagrams shall display information about the core ESInet design, the configuration, the interconnections and the access network links so that the diagram can be used as a basis for evaluation and understanding.

ESInet diagrams submitted shall depict, where appropriate, the following aspects of the proposed ESInet solution:

- Network map(s)/Diagram(s)
  - Logical topologies
  - Physical topologies
- Physical and logical path diversity
- Network ingress and egress points
- Connection types
- Capacities/estimated bandwidth
- Interconnection locations:
  - Node locations
  - Data Centers
  - Aggregation points (both carrier and local access)
- Additional technologies and interfaces as necessary

TCS Response: Comply.

Detailed network diagrams will be made available once a final design and any additional services are confirmed as part of the solution. General network diagrams for discussion and illustration are shown below.

Exhibit 1 shows the logical call paths and transport media in use for the TCS solution.

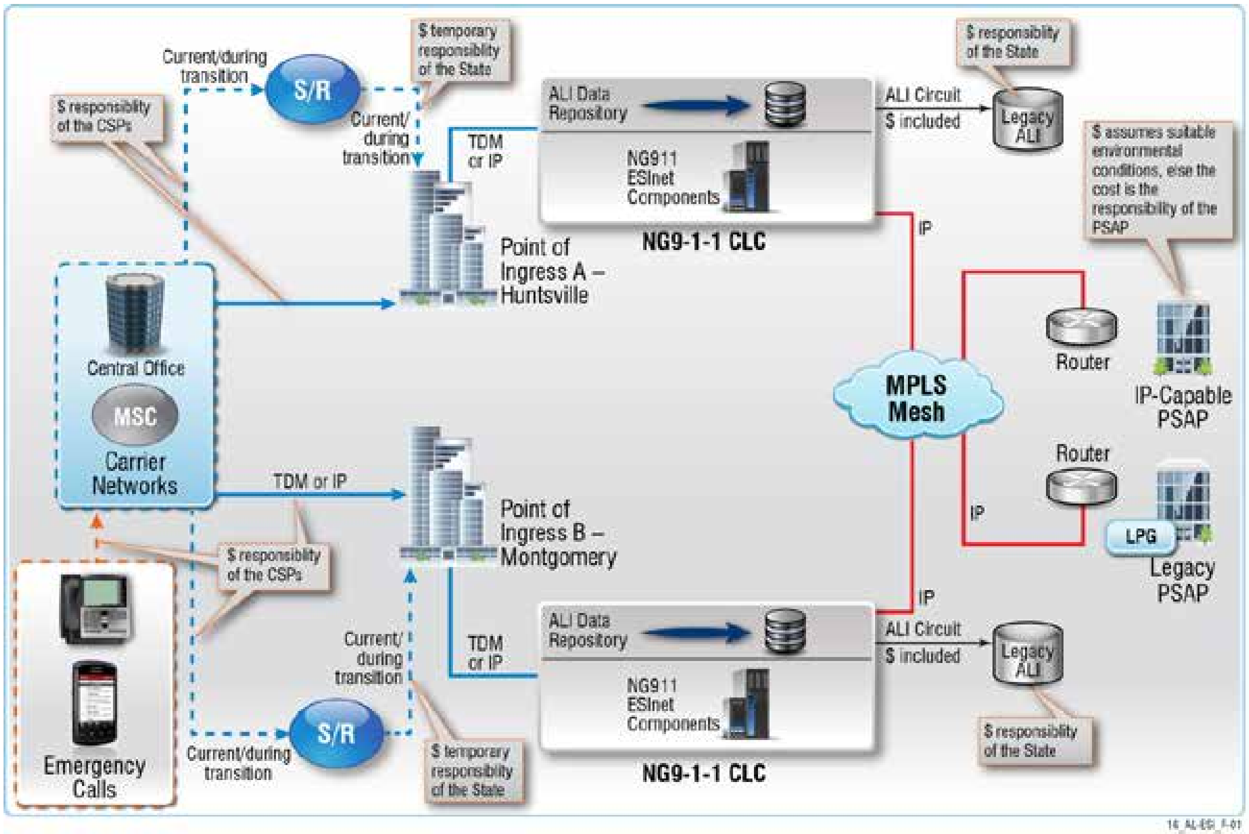
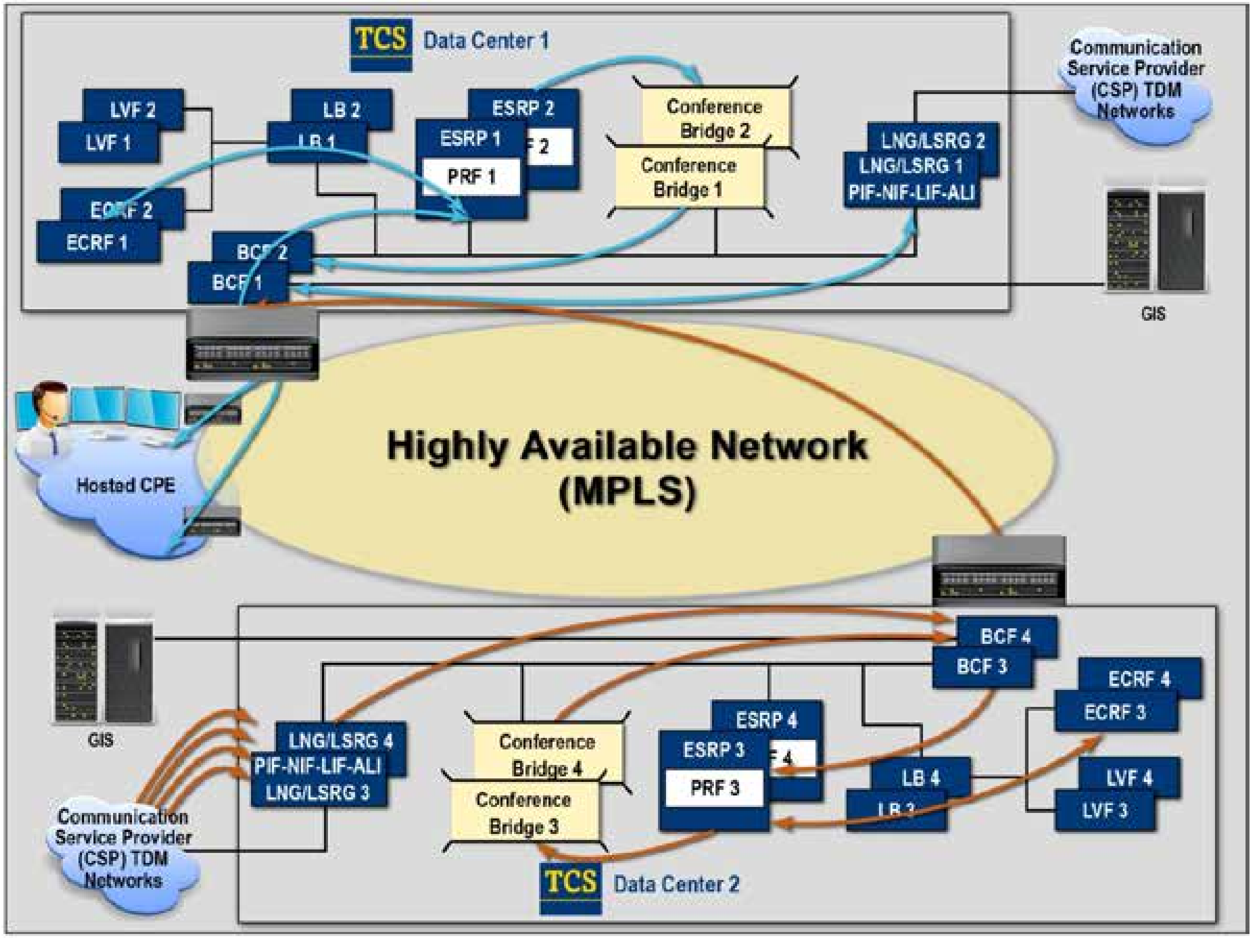

Current/during transition
S/R
$ temporary responsiblity of the State
$ responsibility of the CSPs
Current/ during transition
TDM or IP
ALI Data Repository
NG911 ESInet Components
NG9-1-1 CLC
ALI Circuit
$ included
Legacy ALI
$ responsiblity of the State
$ assumes suitable environmental conditions, else the cost is the responsibility of the PSAP
IP
Point of Ingress A – Huntsville
Central Office
MSC
Carrier Networks
MPLS Mesh
Router
IP-Capable PSAP
Router
IP
LPG
Legacy PSAP
TDM or IP
Point of Ingress B – Montgomery
$ responsiblity of the CSPs
Current/ during transition
TDM or IP
IP
ALI Data Repository
NG911 ESInet Components
ALI Circuit
$ included
Legacy ALI
Emergency Calls
Current/during transition
S/R
$ temporary responsiblity of the State
$ responsiblity of the State
NG9-1-1 CLC
14_AL-ESI_F-01

Exhibit 1. Network Diagram

As can be seen, the aggregation points in Huntsville and Montgomery serve the same function as they do today, which involves collecting all wireless service provider links for those locations. We propose to re-use this existing architecture; the only change has the gateways being replaced with our own LNG components. The remainder of our Intrepid9-1-1 Next Generation Core Services (NGCS) equipment and applications will also be located in the Huntsville and Montgomery data centers—a.k.a. ASA sites or Call Logic Centers (CLCs). We maintain an option to provide application processing from our national data centers in Dallas, Texas, and Raleigh, North Carolina; however, given the sizable nature of the deployment, we would prefer to locate our applications within Alabama.

As shown above, the CLCs are connected to the PSAPs via an MPLS mesh network. We understand there may be an option to reuse the existing T1 network to the legacy selective routers, but we prefer the end-state goal of directly connecting PSAPs through an IP network. This diagram illustrates the redundant nature of the solution from a high-level network point of view.

TCS maintains redundancy inside the CLC as well. Exhibit 2 illustrates how the applications that reside within the CLCs are designed, as well as their logical connections to other network components.



Legend:
- Other emergency call network operators, referenced as Communication Service Providers (CSPs), connect to LNG/LSRG(s) over redundant and diverse connections.
- External access to the ESInet requires a minimum of two points of interface.
- LB means Load Balancer

14_SD911_O_F-02

Exhibit 2. Application Redundancy Diagram

Additional documentation will be provided as needed for discussion and, ultimately, to document the system as it has been built.

2.4 ANGEN ESINET FEATURES AND FUNCTIONS

Respondents shall provide a narrative of their proposed ESInet with enough detail to ensure proper evaluation, using diagrams to provide an appropriate level of detail and common language that explains how their proposed ESInet solution is capable of supporting legacy 9-1-1 network options, NG9-1-1, current and evolving standards, and how it will accommodate the integration of other networks operated by other providers that comprise the ANGEN ecosystem.

The narrative will address each of the features or functions listed below (in no particular order):

1. Operations
2. Security (both physical and logical)

3. Availability
4. Monitoring
5. Alarming
6. Maintenance
7. Disaster Recovery
8. Service restoration
9. Outage mitigation
10. Core routing
11. Interface to Hosted solutions
12. Fault zone design methodology

Respondents shall provide a list and a description of all protocols or routing functions that are used in the ESInet infrastructure and ensure that they conform to NENA Detailed Functional and Interface Standards for the NENA i3 Solution NENA STA-010 standards. The proposed ESInet solution must be aligned with NENA 08-003 to ensure that the proposed network does not conflict with open standards specifications.

Respondents shall provide the system narrative immediately following this Section 2.4. Additional requirements and specific technical specifications are detailed in Sections 2.4.1 – 2.4.13

TCS Response: Comply.

The below narrative illustrates the design concepts in our solution, which is based on the NENA i3 vision of an ESInet and its supporting services. In addition to the narrative, we have provided Exhibit 3 as a summary of the specific points to be addressed in Section 2.4.

Exhibit 3. ESInet Features and Functions

Requirement	Methodology
Operations	Operated by TCS engineers directly. TCS has 19 years of experience managing both E9-1-1 and NG9-1-1 deployments, and we currently process more than 200,000 9-1-1 calls per day via our applications.
Security (both physical and logical)	We maintain a dedicated security staff and have deployed a variety of security measures that are equal or better to NG-SEC and other industry-normal requirements. We have a SIEM system deployed to monitor security events, and we operate our ESInets as closed networks with controlled port access and strict firewall rules.
Availability	Our NG9-1-1 services maintain 99.999% availability
Monitoring	Conducted 24x7 from TCS facilities in Seattle, Washington, and Phoenix, Arizona.
Alarming	Using a customized deployment of HP and Remedy software, our alarming is conducted from our NOC, where it is triaged as necessary.
Maintenance	We use an extensive change control process known as an IBOP (Installation and Back Out Plan) for all maintenance activities.

Requirement	Methodology
Disaster Recovery	We maintain a disaster recovery and business continuity plan book, both physically and electronically, to ensure we have comprehensive plans in place.
Service restoration	We maintain an Incident Management Plan to both communicate and resolve all service-impacting issues.
Outage mitigation	Our active–active design limits outage impacts, as there is no manual intervention required upon the loss of a site or an application.
Core routing	Our applications are designed to automatically mitigate outages, with extensive re-routing and alternate-routing capabilities built into the logic.
Interface to Hosted solutions	We include the necessary interfaces for visibility into our hosted solution. Such interfaces may include—where applicable—ALI data query ability, trouble-ticket query ability, network availability, and other observation tools.
Fault zone design methodology	Our redundant sites strive for the greatest practical physical diversity. The sites in Huntsville and Montgomery offer decent diversity, and out-of-state options are available if preferred.

Intrepid9-1-1 Call Routing Components

Intrepid9-1-1 is composed of the following National Emergency Number Association (NENA) i3-compliant components: a NENA i3 Legacy Network Gateway/Legacy Selective Router Gateway (LNG/LSRG), Emergency Services Routing Proxy (ESRP), MIS system, and emergency call routing function (ECRF)/location validation function (LVF), and their respective sub-systems.

LNG/LSRG

The Intrepid9-1-1 Legacy Network Gateway (LNG) / Legacy Selective Router Gateway (LSRG) provides location by value, populating the Presence Information Data Format – Location Object (PIDF-LO) within the SIP messaging with the full location of the caller via interaction with whatever legacy Automatic Location Identifier (ALI) Database Management Systems (DBMS) infrastructure may exist. This interaction is performed to NENA i3-compliant solution specifications. Also, Intrepid9-1-1 is capable of submitting queries to a NENA i3-compliant external Location Information Server (LIS), once those solutions enter the marketplace. Intrepid9-1-1 communicates with a Border Control Function (BCF) to secure such interconnectivity and subsequent messaging. Furthermore, Intrepid9-1-1 can provide location using a de-reference protocol against an external third-party LIS infrastructure.

The TCS solution can exist in a number of routing states, depending upon the transitional maturity of an overall NG9-1-1 system. For example, our Intrepid9-1-1 IP-based ESRP can deliver calls to legacy PSAPs and NG9-1-1 PSAPs. The company’s IP-based call-handling solution can accept calls from legacy selective routers or NG9-1-1 selective routers. The only changes involve the type of equipment (routers, switches, and gateways) to be installed at each respective location, and whether analog signaling is being converted to SIP, or if SIP signaling is being converted to analog.

The system currently supports the delivery of direct SIP, Signaling System 7 (SS7), analog Centralized Automatic Message Accounting (CAMA), T1 CAMA, Primary Rate Interface (PRI)/Integrated Services Digital Network (ISDN), Plain Old Telephone Services (POTS), SIP, and Private Branch Exchange (PBX). In the event a call taker is still using a legacy system, the call is converted back into analog format at the PSAP level.

The Legacy Network Gateway is made up of three functional components, the LIF, NIF and PIF, all of which comply with LNG/Legacy Selective Router Gateway (LSRG) functions as described within the NENA i3 standard.

Component 1 – PIF: The Protocol Interwork Function (PIF) is contained within a single device that maps inbound TDM fields sent via call signaling to the appropriate SIP fields. The PIF is fully compliant with RFC 3261 and also complies with the unique signaling requirements for 9-1-1 through the use of SS7 ISDN User Part (ISUP) trunk termination. Other versions of the PIF can support both MF and E-MF trunk termination and convert to SIP as well. The preference, however, is to use SS7 trunks for terminating calls originated on the legacy 9-1-1 selective routers. It is therefore imperative that any LNG/PIF be capable of understanding and inter-operating with the signaling from the legacy selective router to provide true bi-directional communications as needed—for example, to support a tandem transfer to some other PSAP. The PIF also interworks the voice media received on the TDM side to Real-time Transport Protocol (RTP) formatted voice media for delivery within the proposed ESInet. In all cases for voice, the PIF shall minimally employ a voice codec of G.711. The embodiment of the PIF is a commonly available off-the-shelf conversion gateway available from a variety of vendors; TCS typically uses the carrier-grade Sonus media gateway, which is the proposed solution here.

Component 2 – LIF: The Location Interwork Function (LIF) shall be co-located with the first-hop destination, which is the ESRP. This component shall be responsible for querying the appropriate location database that is geographically associated with the PIF (whether an ALI or a LIS) with the calling party's Automatic Location Identification (ALI) (as parsed out by the NG9-1-1 Interwork Function [NIF] and described below). In the event an ALI database is queried, ALI steering shall be invoked if a Pseudo Automatic Number Identification (pANI) is presented. In addition, the LIF can provide optional functionality for wireless calls (when required) to directly query an Mobile Positioning Center (MPC)/Gateway Mobile Location Center (GMLC) by using the E2/PSAP-to-ALI Message (PAM)/Mobile Location Protocol (MLP) to obtain wireless location information and then provide the appropriate value and reference for location updates within the SIP signaling, compliant with RFC 4119 as updated by RFC 5491 and RFC 5222.

The logic behind separating the two (PIF and LIF) allows for the greatest flexibility to evolve the service to support carriers who would like to send calls via their own PIF. It also allows for the graceful decommissioning of the LIF in the event it is no longer needed—achieved by simply turning the function off at the ESRP.

Component 3 – NIF: The NIF is also co-located with the first-hop ESRP; its role is twofold. First, it will determine the correct ANI as sent from the PIF and hand that to the LIF for location querying. Second, it will use the resulting location information as provided by the LIF to query the Emergency Call Routing Function (ECRF) with the location information formatted as a PIDF-LO (RFC 4119 updated by RFC 5139 compliant) to include the correct service Uniform Resource Name (URN) and then route the call appropriately. 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. If the information is available, the NIF will also apply additional data about the call.

Flexibility is paramount, and the separation of the NIF from the other functions allows it to use the normal processes for i3-compliant call routing associated with the ESRP. This also allows the proposed architecture to be fully realized for these two functions within the proposed ESInet. For example, if a PIF in Huntsville is unable to send a call to the local NIF/LIF, it will be able to use other deployed groups—for instance, Montgomery—to take the appropriate LNG/LSRG-related actions. This also allows for maximum flexibility for calls delivered to other Point of Ingress/Interconnection (POIs) that may not have connectivity to the appropriate ALI database; the sharing of LIF/NIF functions allows for all sites to maintain geographically local connectivity to all ALI databases and other sources of location information, regardless of which PIF was used to receive the call.

ESRP/PRF

The Intrepid9-1-1 Emergency Services Routing Proxy (ESRP) and Policy Routing Function (PRF) is responsible for coordinating call routing (via ECRF/Location to Service Translation [LoST]) and policy implementation for NG9-1-1 applications per NENA i3. The Intrepid9-1-1 ESRP is the replacement for legacy selective router technology. It interfaces easily with other ESRPs as well as additional Intrepid9-1-1 ESRP implementations, and it can receive and parse Presence Information Data Format - Location Object (PIDF-LO)—both civic and geospatial—per the NENA i3 standard. Location information is embedded in the Session Initiation Protocol (SIP) message header PIDF-LO, also per the NENA i3 standard.

Key benefits include:

- Exceeds the NENA i3 standard for NG9-1-1 call routing.
- Has automatic failover to a redundant backup with no manual intervention, no A/B switching, and no hot standby.
- Bridges the gap from legacy analog (public switched telephone network [PSTN]) with high-quality conversion of call data to IP.
- Routes based upon spatial as well as tabular data.
- Provides a nonproprietary, software-based device that can evolve as technology advances.
- Integrates easily with existing infrastructure and services on the ESInet.
- Offers a highly available, load-balanced and fault-tolerant system.
- Saves money by building a shared ESInet and services with other agencies; integrates with existing Time Division Multiplexing (TDM) infrastructure as well as other ESInets.
- Saves cost with commercial off-the-shelf (COTS) hardware and no future hardware forklift.
- Is easy to install and scalable to future needs, with unlimited trunking capability and no interface cards required.

ECRF

TCS has included its Intrepid9-1-1 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 Alabama's GIS. Attributes provided must meet the minimum Intrepid9-1-1 ECRF specifications, which we will determine with input from Alabama's GIS personnel.

The application server supporting the function is a redundant array of Windows servers running Esri ArcGIS and TCS ECRF software. 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:

- Point data
- Circles
- Arc bands
- Polygons

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

Alabama's GIS data will be loaded onto each ECRF server as part of the equipment staging process. Connectivity to an ArcSDE replica copy 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 Intrepid9-1-1 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.

Intrepid9-1-1 ECRF has built-in audits and error handling that will notify Alabama's systems administrators via GeoComm when data received from the single GIS master database does not meet conformity requirements. Alabama and GeoComm will work directly with the appropriate 9-1-1 entities to make any necessary updates to GIS data. Alabama will then resynchronize updated GIS data to the TCS "auditing" geodatabase via the GeoComm SIF. If data has not passed audit, the workflow described above must be repeated until such data issues have been remedied by the state.

The ECRF/LVF GIS databases will be automatically synchronized at regular intervals with the master GIS database via either Open Geospatial Consortium (OGC) Web Feature Service (WFS) GIS replication or Esri spatial database engine (SDE) geodatabase replication.

The Intrepid9-1-1 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 (Esri data) 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: findService, listServicesByLocation, listServices, and getServiceBoundary
- Support for Esri enterprise and file geodatabases
- Runs on COTS equipment
- Support for errors, warnings, and redirects

LVF

GeoLynx Spatial Router LVF is an IETF 5222 compliant LoST Server that provides the NENA i3 functional elements of ECRF/LVF as specified in NENA TSD 08-003. Functionally, many of the features of the GeoLynx ECRF are also part of the GeoLynx LVF given that both are based off of the same LoST servers. Please see Section 4.8 for additional information.

Legacy CPE Site Interconnection

TCS can provide Legacy PSAP Gateways (LPGs) for interconnection of legacy sites, upon request. If LPGs are required, each legacy PSAP would receive two Mediant 1000 IP gateways, installed with the appropriate number of four-port FXO cards, depending upon how many 9-1-1 trunks are being delivered to the PSAP.

In addition, each PSAP-provided rack will require two 120V 20Amp NEMA L5-20R power connections (provided by the customer) for connecting to the TCS-provided UPS units, which are to be located within three feet of the base of the equipment rack.

At the time of deployment, TCS will provide a 66 Block with a 25-foot Amphenol cable for interconnecting the equipment rack and the telco demarcation/cross-connection backboard.

WAN

TCS will procure and be responsible for network connectivity up to the edge routers in the PSAPs. WAN will typically be provisioned via highly available circuits, such as MPLS, and can be configured for non-redundant, redundant, or redundant/diverse circuits, as required. For Alabama we have provided a non-redundant quote for MPLS service.

Intrepid9-1-1 ALI Service

Our Intrepid9-1-1 service offers ALI for 9-1-1 systems. It provides ALI to legacy automatic number identifier (ANI)/ALI controllers and acts as a link between those controllers and ALI databases to offer levels of functionality not available on most ANI/ALI controllers. It also provides support for multiple database connections as well as connectivity to wireline and wireless database suppliers.

By allowing for ESInet-wide awareness, the location interwork function (LIF), facilitated by the TCS Windows-based service, can query any ALI database connected at any point to any of the downstream end-points. As a result, misrouted calls to a particular end-point do not impact the ability to obtain the proper ALI from any interconnected database for call processing.

In the absence of any useful location information for call routing, the NG9-1-1 interwork function (NIF) applies default routing rules based on the trunk type and/or location of the protocol interwork function (PIF). These rules help to establish the next hop ESRP, where policy rules via the PRF can then be applied to the call as well.

ALI Database Replacement Solution Summary

The legacy Automatic Location Identification (ALI) system is an integral part of the Enhanced 9-1-1 (E9-1-1) environment. Address information for an inbound call is retrieved from the ALI and displayed to the call taker. The Master Street Address Guide (MSAG) is used to format the information and as a validation source whenever new subscriber accounts are added. The evolution of E9-1-1 to NG9-1-1 has resulted in the replacement of legacy ALI and MSAG databases, but the transition must be carefully managed. TCS' Intrepid9-1-1 ALI replacement solution manages current ALI/MSAG challenges while preparing for the transition from legacy ALI/MSAG to NG9-1-1 in the following ways:

- Controlling Recurring Maintenance Costs—TCS has engineered a solution that is both highly reliable and cost-effective to ensure a smooth and reliable transition.
- Preparing for the Use of GIS Data—The TCS ALI replacement solution optionally allows for the use of GIS data as the source for call routing without affecting carrier input processes or ALI functionality. Through the careful management of GIS input data, TCS

can format MSAG-like records for use in the Service Order Input (SOI) provisioning process such that Communication Service Providers (CSPs) can continue with their current SOI methods.

- Support of Legacy E9-1-1—The NG9-1-1 features and their benefits are superior to legacy E9-1-1 features, including in the replacement of the ALI database. However, TCS recognizes the need for replacement ALI services prior to the deployment of NG9-1-1 and Intrepid9-1-1 supports a legacy ALI DBMS (Data Base Management System) to address current E9-1-1 deployments while preparing for the move to NG9-1-1.

Solution Assumptions

The following assumptions baseline the ALI replacement product. Given the inherently flexible nature of the TCS solution, however, these assumptions should be taken as they are intended, as a starting point for a full-solution architecture.

- TCS assumes the state of Alabama desires a legacy ALI replacement product. If the state prefers subscriber data to reside in the NG9-1-1 database, TCS can include a LIS/CIDB as part of its solution that houses all the subscriber data. However, LIS/CIDB products are outside the general scope of this proposal.
- The TCS ALI replacement solution is configured to manage either MSAG or GIS-based data.
- For a GIS-based solution, TCS assumes the jurisdiction has a master Geographic Information System (GIS) database in place with the necessary layers of GIS boundaries, including PSAP boundaries, law enforcement agency boundaries, fire service area boundaries, and medical service area boundaries.
- The TCS NG9-1-1 services will be provided as a hosted model such that TCS maintains ownership of all hardware, software and other service components.

Features of the TCS ALI Replacement Solution

TCS has structured the ALI replacement solution to utilize a percentage of the NENA-defined i3-compliant components and processes in NG9-1-1. However, as a transitory step, the state of Alabama may best be served by a more traditional 9-1-1 ALI solution, with processes that support NG9-1-1.

Intrepid9-1-1 delivers a combination of a traditional ALI and its processes, which are needed today, coupled with those NENA i3-compliant components and processes that are currently applicable. The jurisdictions, local agencies, TCS, and service provider stakeholders can put the building blocks in place to add additional services as 9-1-1 stakeholders move into the NENA i3 space and/or as the state of Alabama feels i3-leaning changes should be made.

TCS meets current and future ALI database challenges through its Intrepid9-1-1 ALI replacement solution, comprised of ALI DBMS and ALI Web products, as outlined below in Exhibit 4.

Exhibit 4. ALI DBMS Features

Feature	Intrepid9-1-1 ALI Support
Daily Audits	X
Performs Rigorous Validation Checks on Service Orders and Manual Edits	X
NG9-1-1 Aligned	X
Enables GIS Data Source Inputs	X
Provides Access for Error Review, Statistics, and Reporting	X
Supports Service Provider Batch Edits	X
Allows Service Providers to Submit Change Requests Directly to ALI DB	X
Automated MSAG-Like Data Management Tools	X
Supports Community and Street Name Aliases	X
Provides Each Service Provider with TN Record Downloads for Data Quality Assurance	X
Provides Administrators with Full History for All TN and MSAG Records	X
Web-Based Reporting Tools	X
Built-In Data Audits	X
Service Order Fallout Reporting	X
Import/Export Standard NENA Formats	X

2.4.1 VOLUME AND PERFORMANCE

The ESInet shall be designed to handle, at a minimum, 4,000,000 calls annually, and an estimated 1,000,000 emergency text messages (inbound and outbound) initially.

The wireless traffic high month was 6,617 hours of talk-time.

The ESInet shall be capable of increasing capacity by 10 percent annually over the initial term of the contract.

TCS Response: Comply.

The TCS solution is designed to accommodate the above-listed metrics. All applicable ESInet components are scalable by at least 10 percent annually, but are quoted at the initial required volume for cost considerations.

2.4.2 NETWORK AVAILABILITY & RELIABILITY

The proposed system, including all subsystems, shall be available a minimum of 99.999% of the time when measured on a 24x7x365 basis during a calendar year. Respondents must provide a description of how the availability and reliability will be measured and include a Service Level Agreement (SLA) that is consistent with the recommendations of ESIND and NENA08-003.

Respondents shall explain how the system will achieve this level of availability.

TCS Response: Comply.

The TCS solution is designed to accommodate five-nines reliability (99.999%) on a calendar year basis.

Network Service Level Agreement (SLA)

It is our expectation that the network would be configured to provide a minimum of 128 Kbps per voice call; also, all calls should use the G.711 Codec, which offers the highest possible call quality as measured against other compressing codecs. This is double the bandwidth that “carrier grade” voice calls are provided; it is necessary to double this bandwidth to ensure accurate voice retransmission and maximum system reliability.

We observe average interface utilization, as it relates to a broadband connection over a specific period of time, to ensure that any one particular interface does not exceed a specific value (predetermined jointly); we typically view top usage interfaces only.

Quality of Service (QoS)

Voice traffic is prioritized at Layer 3 through the use of DSCP. All voice traffic associated with this solution receives a DSCP hex code that is defined on the routers and provided priority queuing.

We primarily recommend the use of Cisco IOS Access-lists (ACL)—or their equivalent, as dictated by network infrastructure—to specify network traffic behavior. Once defined, we then recommend the building of policies to control this routing methodology. Our recommended policies typically provide preferential treatment in the following order:

- Voice (including SIP messaging) and associated messaging
- SQL
- Everything else

"Everything else" is provided treatment using Class Based Weighted Fair Queuing (CBWFQ).

The Layer 2 network that allows for traffic shaping (e.g., MPLS) prioritization should typically be provided for in the following manner:

- 7 – Voice
- 6 – Everything else

If offered in this manner, all QoS options are available on a per-connection basis, as well as on a per-traffic type.

Coupled with Layer 2 traffic control, private line access offers superior data delivery when compared to other mechanisms. MPLS transport also offers an SLA for packet delivery, latency and jitter for all traffic. Exhibit 5 shows the specific latency, packet delivery, and jitter requirements that should be met on the provided network.

Exhibit 5. Network Specifications

Specification	Value
Latency	50ms average, node-to-node delay
Packet Delivery	99.5% packet delivery, average port-to-port
Jitter	2ms average, node-to-node

Jitter Mitigation

The solution will include configurable jitter buffers at the following nodes:

- **Gateway:** The gateway allows for up to 40ms of compensation for traffic that has arrived un-sequenced, out of sequence, or fragmented. This buffer allows for the correct sequencing and delivery of packets to the network.
- **ESRP:** The adjustable input on the ESRP application allows for the correction of jitter-related maladies that occur on the network. The theoretical limit to this buffer is upwards of 30ms.

In all cases, increasing the jitter buffer size adds to the delay of voice delivery over IP to the call taker. As a rule, total jitter buffer delay should never exceed 70ms. As a result, it is important to ensure that initial steps to alleviate jitter on the network are addressed before contemplating the adjustment of buffer default values.

Mean Opinion Score

Based on the aforementioned mitigation techniques, Exhibit 6 lists mean opinion scores to be expected for each implementation of different Codec types.

Exhibit 6. Mean Opinion Score by Codec

Codec	Data Rate [kb/s]	Mean Opinion Score (MOS)
G.711	64	4.3
G.729	8	3.92
G.723	6.3	3.9
G.729a	8	3.7

The NENA i3 solution requires an end-to-end G.711 Codec; it is therefore imperative that an end-to-end MOS test should generate at least a MOS rating of 4.3.

2.4.3 INTERCONNECTION OF OTHER NETWORKS AND SYSTEMS

The proposed solution must be designed to allow for interconnection to other ESInet implementations, PSAP systems (CAD, logging recorders, etc.), criminal justice networks, other 9-1-1 networks or other secure public safety technologies as may be designated by the Board. The proposed solution must ensure “open standards” and describe provisions to collaborate with potential interconnected solutions.

Respondents shall describe the ability for their ESInet solution to interconnect and interoperate with other ESInet implementations, PSAP systems (CAD, logging recorders, etc.), criminal justice networks, other 9-1-1 networks or other secure public safety technologies as may be designated by the Board.

Any IP network approved by the Board to connect to the ESInet shall be required to comply with appropriate ESInet, NENA, and National and Open Standards described in this proposal or as may be current at the time of proposed interconnection.

The ESInet shall be configured in a manner that Board approved edge site Local Area Networks (LANs), such as computer aided dispatch (CAD) systems and/or other Public Safety systems may be connected to utilize the functionality created by the ESInet.

Respondents shall be accountable for ensuring that additional networks meet the minimum qualifications for interconnection presented in this specification and that security of ANGEN is maintained through collaboration with each potential network provider.

TCS Response: Comply.

We support the industry vision of a "network of networks." In order to accommodate this vision, a number of different types of interconnections are required.

Our design philosophy for Local Area Networks (LAN) interconnection is to use logically separated networks to ensure proper data handling. We also typically design for a "closed" network (i.e., no connectivity to the public Internet or any other subnet) except for secure anti-virus updates, if applicable. Interconnections with other LANs introduce risk, but we manage that risk with the appropriate use of logical network separation and firewall devices to ensure that 9-1-1 data delivery remains a closed system.

Additional Ethernet interfaces can be used on the router/firewall combination for auxiliary networks. Exhibit 7 illustrates the auxiliary network connections.

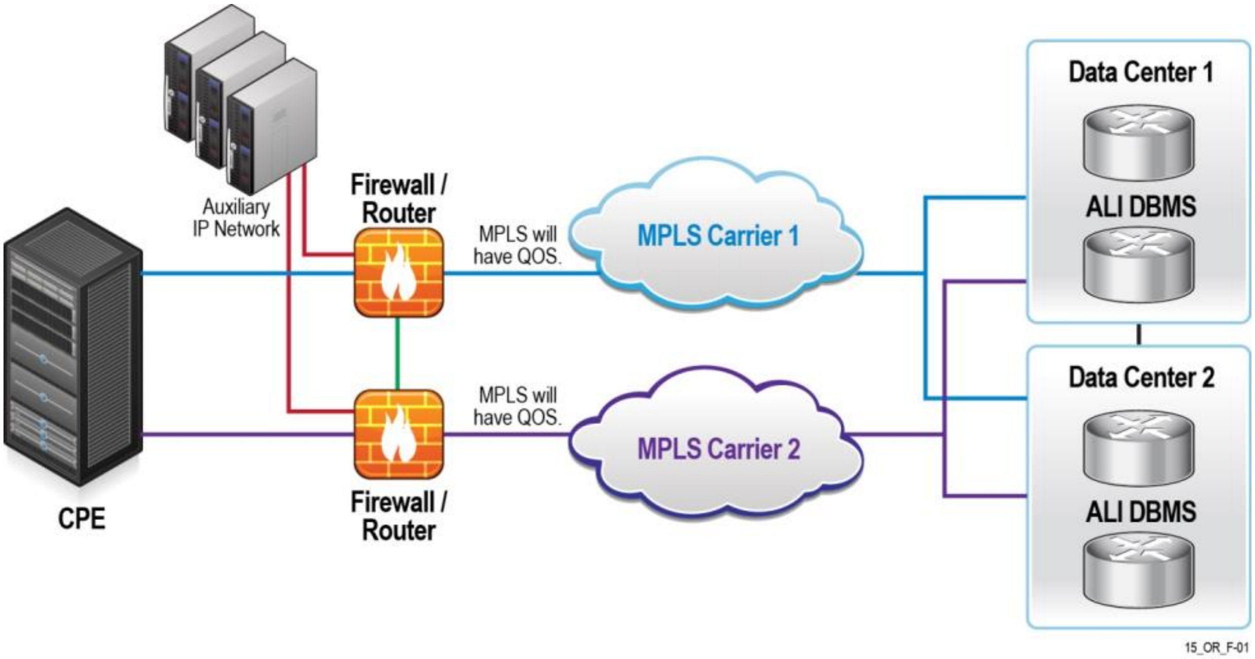


Exhibit 7. Auxiliary Network Connections

Interconnections with other ESInets will be accomplished through SIP messaging and transfers between ESInets. For instance, TCS oversees the ESInet in neighboring Tennessee, which will ease the transition to the ESInet in Alabama when it comes to transfers into that network.

We note that ESInet-to-ESInet communication is not yet common. We typically interconnect with other networks for transfers through an existing selective router network. We will deploy a LSRG (Legacy Selective Router Gateway) as part of this proposed solution. The LSRG contains the protocols and intelligence to convert a SIP/RTP call to a SS7/ISUP call for transfer to an existing selective router. As selective routers continue to be replaced with IP solutions, this conversion will become less frequently needed and will eventually become obsolete.

2.4.4 QUALITY OF SERVICE FEATURES

Any proposed ESInet shall have quality of service (QoS) features suitable for the real-time transport of VoIP traffic requesting emergency services (as defined in NENA 08-003).

Respondents shall describe their method of managing the QoS features defined below and offer an explanation of how their proposed ESInet will perform to these capabilities

The following ESInet performance requirements are taken directly from NENA 08-506 ESIND:

1. Packet Latency (50 ms)
   - Packet Latency shall average a round trip time of fifty (50) milliseconds.
2. Packet Loss (5%)
   - Respondents shall design the ESInet without oversubscription and keep the packet loss budget under 5%.
3. Jitter (20 ms)
   - Jitter shall not exceed twenty (20) milliseconds.

Respondents shall provide an explanation of the proposed solutions QoS capability that minimizes congestion, mitigates errors and ensures the delivery of Real-Time Transport Protocol (RTP) packets across the ESInet.

TCS Response: Comply.

Voice traffic is prioritized at Layer 3 through the use of DSCP. All voice traffic associated with this solution receives a DSCP hex code that is defined on the routers and provided with priority queuing.

We primarily recommend the use of Cisco IOS Access-lists (ACL)—or their equivalent, as dictated by network infrastructure—to specify network traffic behavior. Once defined, we then recommend the building of policies to control this routing methodology. Our recommended policies typically provide preferential treatment in the following order:

- Voice (including SIP messaging)
- SQL
- Everything else

"Everything else" is provided treatment using Class Based Weighted Fair Queuing (CBWFQ).

The Layer 2 network that allows for traffic shaping (e.g., MPLS) prioritization should typically be provided for in the following manner:

- 7 – Voice
- 6 – Everything else

If offered in this manner, all QoS options are available on a per-connection basis, as well as on a per-traffic type.

Coupled with Layer 2 traffic control, private line access offers superior data delivery when compared to other mechanisms. MPLS transport also offers an SLA for packet delivery, latency, and jitter for all traffic.

2.4.5 TRAFFIC PRIORITIZATION NARRATIVE

Respondents shall describe how their proposed solution manages the prioritization of traffic across the ESInet, how QoS is implemented and describe the interoperability of the IP routing mechanisms.

TCS Response: Comply.

The goal of QoS is to guarantee call quality and/or performance. Without the implementation of QoS, PSAPs could possibly experience echo, dropped calls, choppy audio, and poor overall quality. This is unacceptable as it negatively impacts the PSAPs. In a converged environment, all types of traffic travel over a single transport infrastructure. Yet all traffic types are not the same. Data is "bursty" (fluctuates widely), sometimes loss tolerant, and not latency sensitive. Voice, on the other hand, is non-bursty, is not tolerant to loss, and is latency sensitive. The challenge involves providing the required level of service for each of these traffic types. Running both voice and data on a common network requires the proper QoS tools to ensure that the delay and loss parameters of voice traffic are satisfied. These tools are available as features in IP phones, switches and routers.

To design and implement a network that supports mission-critical data and voice, basic tools must be used in order to provide an environment that can ensure voice quality over a data network. The following are the three important steps and tools in implementing QoS in a network.

- Classification
- Queuing/scheduling/policing
- Network provisioning/bandwidth planning/shaping

All three steps will be used within the network that is expected to differentiate between normal data traffic and high-priority traffic, such as voice.

2.4.6 SCALABILITY

The Board seeks a solution that will accommodate bandwidth changes, additional sites to be added or sites removed, and to interconnect to other regional or statewide ESInets without downtime or substantial increase in operating costs.

Respondents shall describe how their proposed ESInet design permits scalability.

TCS Response: Comply.

TCS designs all its systems to be modular and fully scalable. We can scale with respect to bandwidth, additional sites, new technologies, and network interconnections, all without wholesale "forklift" upgrades. As correctly stated in the requirement, some additional incremental cost is to be expected as the network scales, but wholesale replacement of equipment will not be necessary.

2.4.7 REDUNDANCY AND SURVIVABILITY

The ESInet shall be configured to survive natural or man-made disasters at every core site (Central Office, Point of Presence, Data Center or other central switching location) and shall provide a description of survivable capabilities at all edge sites including PSAPs

Additional requirements for the reliability design of the ESInet shall be guided by the FCC Report and Order FCC 13-158 – Improving 911 Reliability and Reliability and Continuity of Communications Networks, Including Broadband Technologies.

Where available, the ESInet network core solution and redundantly connected sites shall include physically diverse routes and physically diverse building entrances.

Respondents shall provide a detailed description of all single points of failure or specific locations that lack diversity and/or redundancy present within their proposed solution. This includes locations within the proposed ESInet where redundant components, network resources and physical connections DO NOT exist.

Respondents shall explain in detail the redundancy and survivability measures proposed for the ESInet and the core network components.

TCS Response: Comply.

We design our systems with complete redundancy. Critical infrastructure will exist in the ASA data centers, as well as in our own CLCs for monitoring and maintenance. The data centers make up the majority of the Intrepid9-1-1 solution. The CLCs will house the applications (e.g., ESRP/PRF; ECRF/LVF; SIF; logging and informational databases; security, monitoring, and portal applications), and Time-Division Multiplexing (TDM) ingress points will be similarly located as part of the LNG at the CLCs.

All TCS safety and security technology—including Intrepid9-1-1—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; 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 Alabama our highly available NG9-1-1 system that can operate 24x7 as a true production system. Our Intrepid9-1-1 architecture has four main 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 in Seattle and Phoenix—will provide some of the system applications and network monitoring services. 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. Locally, the Huntsville and Montgomery ASA sites offer site redundancy as well and will house the remainder of the solution.
- **System redundancy.** We configure our systems for "active–active" call processing. By designing each system node to distribute traffic in the active–active manner, our CLCs effectively load-balance traffic. Engineering the systems in this way also ensures that no failover is required during a catastrophic event that may occur in any one location.
- **Network redundancy.** The state will receive system and network monitoring services that are supported by two different Synchronous Optical Network (SONET) ring providers in Seattle and Phoenix. 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 Intrepid9-1-1 system, combined with both local and geographic redundancy for all production processes, so that no fewer than four servers support any one TCS software service.

In summary, TCS implements local redundancy with separate entrance facilities (when available), 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.

2.4.8 BANDWIDTH

Respondents shall identify the minimum bandwidth required to handle all anticipated voice and data traffic of the system for the next five (5) years.

At a minimum Respondents shall base their bandwidth estimates on the delivery of all calls and associated data to the PSAP.

In addition, the bandwidth should include requirements for a fully functioning network with all redundant connections in service.

TCS Response: Comply.

The Wide Area Network (WAN) will be configured to provide a minimum of 128 Kbps per voice call. All calls use the G.711 CODEC. This is double the bandwidth at which “carrier”-grade voice calls are provided. It is necessary to double this bandwidth to ensure utmost reliability and accurate voice retransmission.

2.4.8.1 PSAP BANDWIDTH

Respondents shall provide a solution that can deliver adequate bandwidth to each PSAP for 9-1-1 voice calls, text to 9-1-1, data communications, and a sufficient surge factor. The growth factor used must conform to the current ANGEN model.

The minimum access portion of the network from the ESInet to the PSAP shall be 10 Megabits per second (Mbps).

Respondents shall continually monitor the bandwidth for the duration of the contract and dynamically increase the bandwidth when appropriate. The selected vendor will be required to supply a SLA consistent with the existing ANGEN solution. A description or sample of the SLA must be included in the response.

TCS Response: Comply.

We will comply with the requirement for 10 Mbps to the PSAP sites, assuming the option to provision a MPLS network is selected to replace the existing T1 and CAMA transport network. We note that this bandwidth may be excessive for some sites and a reduction in bandwidth would allow for some cost savings. Regardless of capacity, all circuits are continuously monitored for performance, and bandwidth increases will be recommended as necessary as a result of this monitoring.

Please see sample SLA in Section 6.3.

2.4.8.2 BANDWIDTH EXPANSION

The ESInet must be capable of expanding as needed throughout the duration of the contract period.

TCS Response: Comply.

Bandwidth is scalable to accommodate the required growth potential of the network.

2.4.8.3 BANDWIDTH SHARING

Respondents shall describe how their QoS scheme ensures that separate RTP sessions are not sharing bandwidth.

Since the ESInet may be used for additional services, respondents must provide a description of how bandwidth is prioritized and separated from normal IP traffic.

TCS Response: Comply.

We will design the solution to use dedicated production links and appropriate routing protocols, in conjunction with application layer controls, to ensure the best path. We typically pair identical bandwidth paths on redundant connections.

Voice and signaling are given the highest priority traffic marking to ensure 9-1-1 calls are urgently delivered.

2.4.8.4 LOSS OF BANDWIDTH

Respondents shall configure the dynamic routing protocol to prevent serious loss of bandwidth, denial of service due to routing table updates or other behavior while providing automatic rerouting as quickly as is reasonably possible.

TCS Response: Comply.

Routing protocols are configured with appropriate timers to mitigate instability anomalies such as faulty devices or unstable connectivity.

2.4.9 IP ROUTING

The Board requests that Respondents propose the most efficient and effective IP routing solution that meets the intent of this RFP.

As the transition from IP version 4 (IPv4) and IP version 6 (IPv6) is on-going, the proposed IP network infrastructure shall be configured to support and route both IPv4 and transition into IPv6.

Respondents shall describe how their ESInet configuration meets an ability to associate IPv4 and IPv6 in a seamless routing configuration.

Respondents must also describe how a combined IPv4 and IPv6 platform will be managed and monitored to avoid potential errors.

TCS Response: Comply.

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—including all third-party components—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. At some point during calendar year 2016, the TCS solution will be system-engineered and certified to operate in an IPv6 environment.

2.4.9.1 INTERNET PROTOCOL PACKET DELIVERY

Respondents shall ensure that the IP routing protocol used in the ESInet provides delivery of IP packets from end to end. All IP information from one IP device to another IP device within the network must be guaranteed.

TCS Response: Comply.

We will work with the state of Alabama's engineers to ensure appropriate ESInet addresses are properly advertised within the route tables.

2.4.9.2 IP ROUTING PROBLEM RESOLUTION

Respondents shall describe how their proposed solution will interoperate with other operators of interconnected networks and will cooperate with those providers to resolve IP routing problems.

The selected vendor will be responsible for ensuring that discrepancies or deviations from standards within the respondent's network are documented and corrective action taken to overcome conflicts with other operators.

TCS Response: Comply.

We will work with interconnected networks and their suppliers on behalf of the state.

2.4.9.3 AUTOMATIC INTERNET PROTOCOL REROUTING

Respondents shall describe how their proposed solution minimizes the impact of routing errors within the network by automatically rerouting past failures or interruptions.

TCS Response: Comply.

We use Border Gateway Protocol (BGP) in conjunction with multiple carriers to supply automated routing functionality in the event of a failure at a network facility. This process is built into our hosted data transaction facilities.

2.4.9.4 BACK TO BACK USER AGENT USAGE

Respondents must provide the ability to cross ESInet boundaries to ensure no limitations or dropping of packets. If SIP or RTP traffic needs to cross boundaries the traffic shall be handled by a back to back user agent (B2BUA); a type of session Boarder controller (SBC).

Respondents shall describe where B2BUAs are located within their solution and document the use of B2BUAs in their ESInet. Respondents must include an explanation of how the seamless delivery of traffic can be maintained using SIP and RTP between IPv6 and IPv4 networks.

TCS Response: Comply.

TCS' solution for the BCF, which includes the back-to-back user agent (B2BUA), supports cross-boundary communications. Other than translating between IPv6 and IPv4, the solution does not use Network Address Translation (NAT) for either the anchoring of media at the BCF, for SIP signaling, or HyperText transfer Protocol (HTTP) traffic through the BCF. The BCF interface that communicates with external entities (such as Wireless Service or VoIP Providers) would be assigned public IPv4 or IPv6 addresses.

TCS acknowledges that NAT can be troublesome and recommends that it not be used, as the operational issues encountered have been found to be unnecessarily complicated. The company will work to identify address conflicts and provide IPv4/IPv6 space that will eliminate the overlap.

TCS' solution will support a fully dual-stack ESInet; the dual-stack solution allows IPv4 networks to transition from IPv4 to IPv6 with minimal, if any, interruption. The key to integration success for the TCS solution is to avoid performing NATs between the two addressing schemes, but rather to deliver dual-stacked solutions for both IPv4 and IPv6. The TCS dual-stacked solutions are consistently applied across servers, routers, the SBC, firewalls, and the MPLS network itself. The TCS IPv4 solution will service external networks or nodes that are IPv4-compatible, and the IPv6 solution will service the internal ESInet. The company will employ COTS hardware for each addressing scheme, and TCS will enable dual, redundant, and diverse Domain Name Server(DNS) entries for IPv6 and IPv4. The solution embodies network engineering simplicity and minimizes SIP- and RTP-related issues.

2.4.9.5 SUBNET NUMBER ASSIGNMENTS

The Board may allow the integration of other networks with the ESInet. To avoid potential conflicts for address space, Respondents shall document and provide a report of all subnet address assignments to the Board prior to implementation of the ESInet.

TCS Response: Comply.

We will document subnet address assignments and provide a report as part of the design of the ESInet, to be completed prior to its implementation.

2.4.9.6 NETWORK STATIC ADDRESSING

Respondents shall ensure that static IP address routing is configured at all core network interfaces to avoid IP configuration errors.

TCS Response: Comply.

We will accommodate static IPv6 network address assignments for all major network interfaces.

2.4.9.7 "LOOPBACK" INTERFACE

Respondents shall define an interface to allow for loopback testing within the ESInet. The loopback interface shall be installed at each network element to provide administration functions.

TCS Response: Comply.

We can accommodate static network address assignments for loopback interfaces to each network element capable of IP administration.

2.4.10 DIVERSE NETWORK ENTRIES

The Board requires an ESInet design that incorporates diverse network entries to connection points and PSAPs. The Board recognizes that in several cases there may not be physically diverse entrances into PSAPs.

Where diverse entries are not possible; Respondents shall describe their methodology to implement the most diverse solution possible.

Respondents shall describe their methodology for providing redundancy through the use of diverse network entries where possible.

TCS Response: Comply.

Our proposed call-routing system is designed to view all PSAPs as a single entity. This end-to-end IP-based call-delivery system can deliver calls using pre-established routing configurations, with redundant and/or diverse network paths between any host site and each respective PSAP. While diverse entries are desired, the lack of diverse entrances does not preclude a highly available design.

Using alternate routing, highly-available router configurations, and other measures to increase reliability as described throughout this document, we ensure the network and call paths are as diverse and available as possible.

2.4.11 NETWORK DEMARCATION POINT

Since the ESInet may be interconnected to other ESInets or facilities, Respondents shall establish demarcation points and the physical connection requirements for other operators to connect to the designated demarcation point.

In addition, demarcation between the Access Network facilities that connect an edge site, such as a PSAP site, to the Core Network, meet the Core Network at a point of interconnection (POI).

Respondents shall explain their preferred methodology for establishing network demarcation points.

TCS Response: Comply.

Once the Time Division Multiplexing (TDM) circuit is aggregated, it is terminated on TCS-owned and -operated digital access and cross-connect systems (DACS) at our CLCs and sent to our LNG. This marks the demarcation point between the TDM ingress and IP egress networks. Once in our CLCs, the call location is determined and then routed via Session Initiation Protocol (SIP)/Real-time Transport Protocol (RTP), and ultimately delivered to the call-taking equipment at the PSAP.

At the PSAP we prefer an Ethernet hand-off, but we are able to accommodate other media types of hand-offs as well.

2.4.12 ACCESS NETWORK - EDGE SITE INTERFACE

The edge or PSAP sites should interface via 100 Megabit per second (Mbps) or faster port speed connection.

This interface to the local LAN is not considered a part of the NG9-1-1 network but should be considered as an element of the ESInet infrastructure.

Respondents shall describe the local area network (LAN) interface at each of the edge sites.

TCS Response: Comply.

We prefer an Ethernet handoff and, if available in the area, can request the compliant handoff media for the area.

2.4.13 TIME SERVERS

A time server to synchronize all proposed network resources must be included in the proposed solution.

The time server must be connected to redundant time sources located within the ESInet capable of providing accuracy to 20.0 milliseconds (ms) of true time.

Respondents shall include a system for establishing network time protocol for the network in their proposal.

TCS Response: Comply.

This proposal includes network time protocol servers for synchronizing time across the network.

2.5 ANGEN NETWORK FAILOVER

The proposed solution must contain a network failover function that is capable of recognizing faults and automatically taking measures to avoid the fault. At a minimum the network shall provide for instant switch from failed or degraded components, systems, and networks.

The failover system shall conform to industry standards and shall comply with the other recommended standards presented in this RFP and must embrace open standards to maximize the fail over ability of all components.

Respondents shall describe in detail their methodology both operationally and technically for implementing automated network failover as a component of their proposed ESInet.

TCS Response: Comply.

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.

The proposed solution is designed as a fully redundant system that employs automatic failover so calls will not be lost. Manual intervention is not required.

The proposed solution is reasonably designed 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 as long as the system, as a whole, is still able to transmit and receive data.

In general terms, the proposed Intrepid9-1-1 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 the two geo-diverse data center 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, even under the most challenging of circumstances.

2.6 ANGEN NETWORK SECURITY

Respondents shall propose a solution that meets a minimum level of security as defined by the national standards.

The Board requires that proposed solutions comply with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security policies and practices.

They may be found at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view.

Respondents shall propose how their solution meets these security measures and how they comply with future changes to security measures to ensure that:

- Network operations are not disrupted due to a security breach
- Unauthorized individuals cannot access the network
- Least access policy is applied
- Data theft does not occur
- Monthly assessments of vulnerabilities and frequent scans for malicious activity occur
- Security incidents are documented, risks identified, responded to and mitigated
- Management of security changes are documented
- Security documentation is maintained to aid in forensic audits as necessary
- Security data is maintained as recovered and not modified or deleted

- Intrusion protection and Intrusion detection is implemented throughout the network to eliminate breach of security
- Protection from identify theft occurs

TCS Response: Comply.

TCS complies with requirements established as part of the NENA Security for NG9-1-1 (NG-SEC) standard, NENA 75-001, v1, the standard applied when deploying systems, as well as NENA 08-751 and 02-010. TCS also maintains ISO 27001 certification. Procedures and standards applied through ISO 27001 and NG-SEC controls meet or exceed the Criminal Justice Information Services (CJIS) policies identified above.

Respondents shall include physical and logical security precautions in their proposed solution that meet the minimum criteria outlined above. This includes providing a description of any security based appliances necessary to meet the objectives including:

- Firewalls
- Access Control Lists
- Switches
- Routers
- Intrusion Protection devices
- Intrusion Detection devices
- Specialized Cabling

Respondents shall describe in detail how the proposed network is configured to withstand these attacks and protect the integrity of the entire 9-1-1 system.

TCS Response: Comply.

Our proposed network solution complies with standard public safety network security guidelines as described by NENA and other standards bodies. The network design provides two basic connection-oriented security assurances:

- The connection is private through the use of Advanced Encryption Standard (AES) or better encryption. The keys used for this symmetric encryption are generated uniquely for each connection and are based on certification provided by the i3-compliant PSAP credentialing authority or another trusted entity.

- The connection is reliable, using Secure Hash Algorithm (SHA) as the method for providing message integrity checks.

In addition, access is granted or denied based upon industry-standard user name/password credentialing, where access at any particular level is granted only to those who possess the proper login credentials.

2.6.1 INTRUSION PREVENTION AND DETECTION

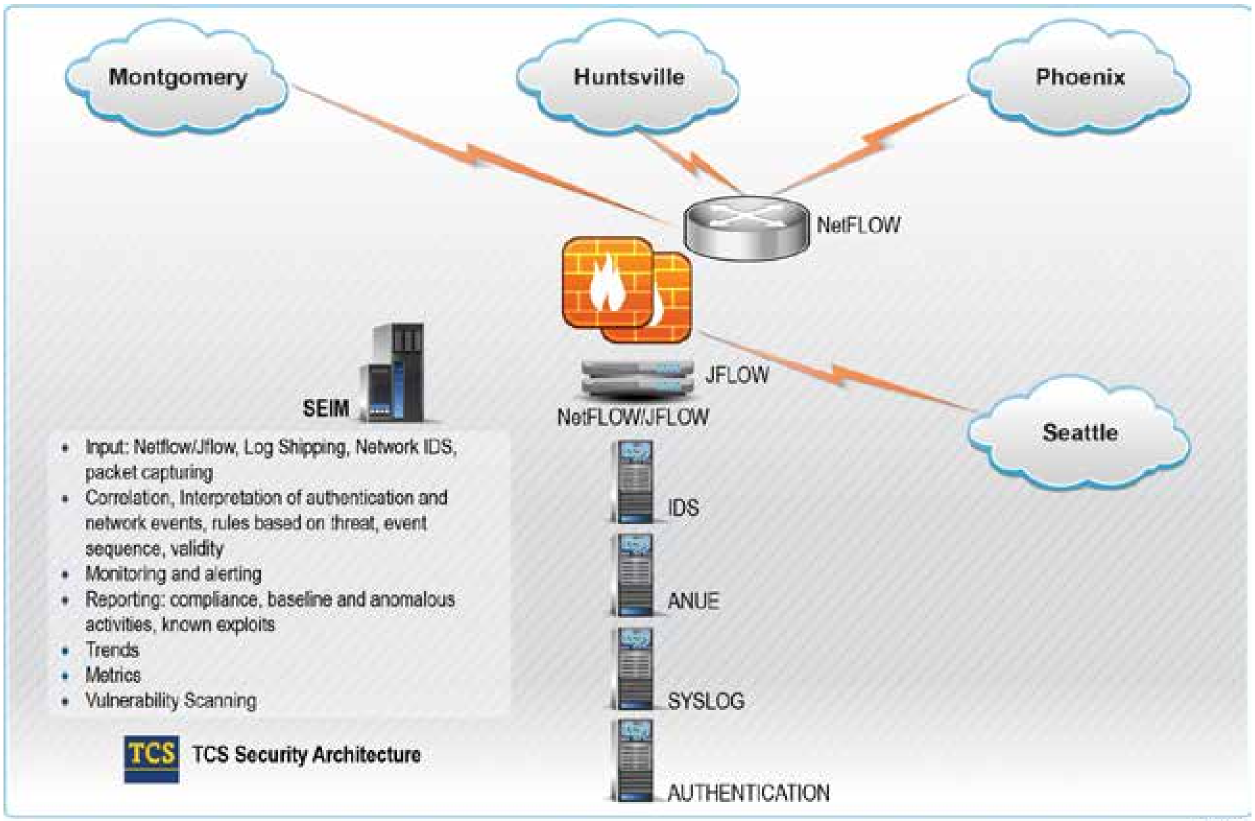
Respondents shall describe how their proposed intrusion prevention and detection capabilities provide alerting, logging and reporting of security threats by intruders to the network. In addition, the ability to document and log intrusions must be discussed within the response.

TCS Response: Comply.

TCS uses an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) appliance. The IDS/IPS appliance provides total packet flow inspection (packet scanning) at wire speed. This means that attacks and exploits applicable to Open Systems Interconnection (OSI) Layers 2–7 are sought out in the packets. The IPS also can block malformed or illegal packets, perform defragmentation and Transmission Control Protocol (TCP) reassembly, and use IP-based access controls. The IDS/IPS filters are vulnerability based so they can be intelligently applied based upon the OS or application environment.

In addition, TCS uses a log event collection system—known as SIEM—to capture all system, IDS and NetFlow data to correlate into incident notification. This system is managed by a dedicated resource.

Exhibit 8 illustrates the TCS security architecture.



- Input: Netflow/Jflow, Log Shipping, Network IDS, packet capturing
- Correlation, Interpretation of authentication and network events, rules based on threat, event sequence, validity
- Monitoring and alerting
- Reporting: compliance, baseline and anomalous activities, known exploits
- Trends
- Metrics
- Vulnerability Scanning

Exhibit 8. TCS Security Architecture

2.6.2 ENCRYPTION

Respondents must include the advanced encryption standard (AES) on their proposed solution where appropriate.

TCS Response: Comply.

Network connections are private through the use of Advanced Encryption Standard (AES) or better encryption. The keys used for this symmetric encryption are generated uniquely for each connection and are based on certification provided by the i3-compliant PSAP credentialing authority or another trusted entity.

2.6.3 NETWORK SECURITY STANDARDS

Respondents shall describe how their network security solution complies with the following Standards:

- NENA Security for Next-Generation 9-1-1 Standard (NG-SEC, document 75-001 dated February 6, 2010)
- Next Generation 9-1-1 Security (NG-SEC)Audit Checklist NENA 75-502 V1
- NENA i3 Technical Requirements Document 08-751
- NENA Detailed Functional and Interface Standards for NENA (i3) Solution Stage 3 08-003
- FBI Criminal Justice Information Services (CJIS) Security Policies
- http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view

TCS Response: Comply.

TCS complies with requirements established as part of the NG-SEC standard, NENA 75-001, v1, the security standard applied when deploying systems.

The TCS Information Security Policy is established to protect the information assets of our organization, customers, and suppliers from all threats whether internal or external, deliberate or accidental, as well as to comply with all governing laws. The intent of this policy is to outline the structure of our Information Security Management System (ISMS) and demonstrate compliance with the ISO 27001 Information Security standard. The ISMS protects the information assets resident within TCS, including information contained within the infrastructure and systems we use for conducting business.

The TCS ISMS is ISO 27001 certified. Industry-leading security standards and best practices are also followed to ensure the integrity and confidentiality of customer and company information in support of our services. These practices include extensive controls in the areas of personnel, systems and facility security.

TCS has a comprehensive physical security program that includes centrally-managed exterior and interior card access controls and video surveillance systems; these are supplemental to standard facility features that include power backup systems, fire control systems, and physical access controls.

The Information Security teams at TCS develop and maintain processes designed to identify new risks and monitor and respond to known security risks. These processes include both process and technical controls such as intrusion detection and prevention systems, ongoing assessment of systems, software, and network environments, and partnering with audit teams to ensure TCS systems and processes are in compliance with information security benchmarks.

TCS maintains a centralized Incident Response Team process with specific criteria for identifying and responding to events in the operational environment, including customer notification, as appropriate. The incident response process is closely integrated with TCS's overall disaster preparedness and emergency response programs. In addition to real-time event management, specific post-event analysis and continuous improvement activities are completed for each incident.

A fully documented, comprehensive disaster preparedness program ensures that all business units have business continuity, disaster recovery, and emergency response plans for critical functions and processes. These are reviewed, updated and tested annually, at a minimum.

TCS is committed to assisting customers in meeting their security goals and audit obligations and will work with account teams and customers to meet those objectives.

2.6.4 REMOTE ACCESS AND NETWORK SECURITY AND FIREWALLS

Respondents shall specify a firewall solution within its network that provides security and protection to the system. All such interfaces connected shall be in accordance with mandated security requirements.

a. Secure remote access shall be strictly controlled. Control will be enforced via remote access authentication using security tokens that provide one-time password authentication or public/private keys with strong pass-phrases.

b. Remote Access control will be enforced via network and system level auditing.

TCS Response: Comply.

In general, our security measures include physical safeguards, OS hardening, hardware and software information security best practices, stringent change management processes, security incident response, educational efforts, and organizational policies.

The firewall component, whether standalone or part of a Border Control Function (BCF), employs all the characteristics normally found in a typical firewall application, including the following elements specific to emergency services network applications:

- Support for Transport Layer Security (TLS) for those originating call entities that request TLS connections, if applicable.
- Port firewalling—Permission for traffic to be allowed only through certain ports opened in the firewall.
- Pinhole firewalling (where applicable)—Ports will be opened to support calls on an individual basis, based upon the requested media port (Real-Time Transport Protocol [RTP]); once the call is completed, the port will be closed again.
- Stateful packet inspection.
- Deep packet scanning—The firewall will work in conjunction with other firewalls that provide a BCF in a common manner so that an attack on one firewall is known by all.

SECTION 3 ANGEN SPECIFIC REQUIREMENTS

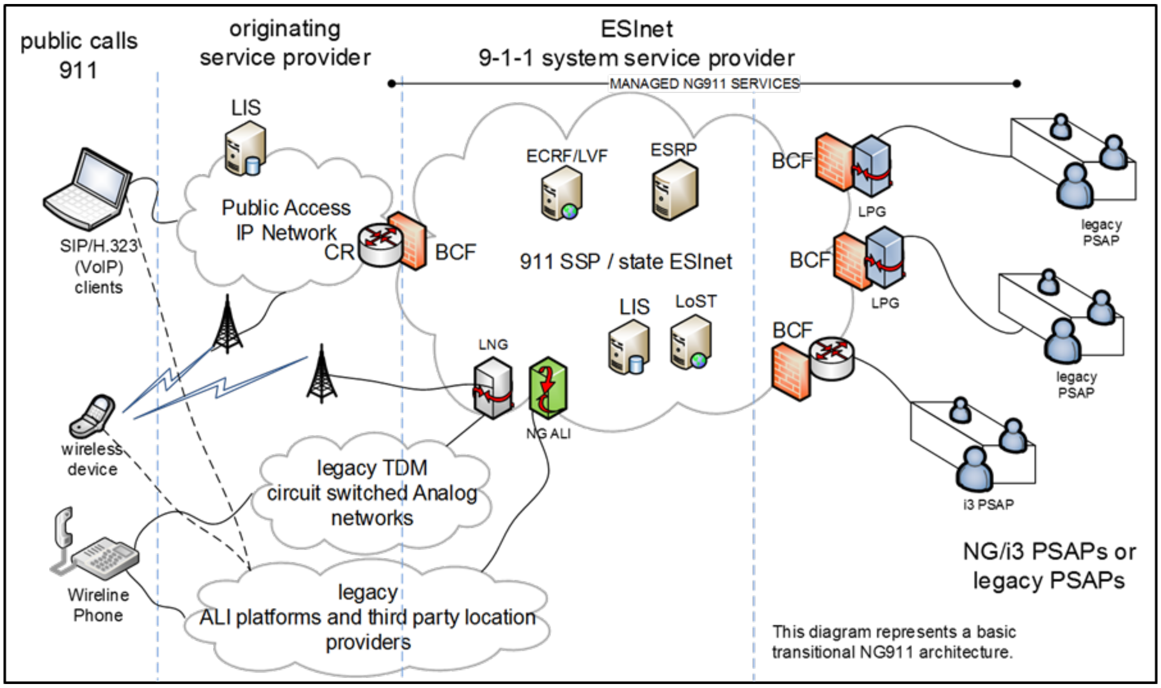


Figure 7 - ANGEN Conceptual Design Diagram

3.1 SYSTEM SERVICE PROVIDER COORDINATION REQUIREMENTS

Successful Respondents will be required to coordinate with other service providers as necessary to operate a seamless solution in support of the operation of ANGEN.

Respondents will need to enter into Interconnection agreements which legally allow the connectivity and interconnection with other networks as well as other service providers throughout Alabama.

This includes but is not limited to LECs, CLECs, ILEC and all Wireless Carriers providing service in Alabama.

Respondents shall provide the Board with example agreements, relationships, licenses or other documents demonstrating Respondents legal ability to enter into such agreements.

Examples of interconnection and cooperative agreements with third parties include but are not limited to:

- pANI (pseudo ANI) and IP provider ALI records integration
- third party providers (TCS and Intrado) E2+ interfaces
- Inter-company ALI server connections (to AT&T, CBT)

TCS Response: Comply.

We have extensive, proven experience as a systems integrator, which requires significant cooperation with outside entities. We will work with all necessary outside entities to implement a successful project.

TCS is currently one of the state of Alabama's third-party providers. Coupled with ALI cooperative agreements that cover approximately half of all wireless calls, and agreements for text delivery for approximately half of all wireless carriers, this illustrates our ability to enter into such an agreement.

3.2 INTERSTATE INTERCONNECTION REQUIREMENTS

Respondents must be capable of interconnecting with other SSPs in states other than Alabama.

States that will need to be interconnected to ANGEN include:

- Florida
- Georgia
- Mississippi
- Tennessee

Respondents shall provide the Board with example agreements, relationships, licenses or other documents demonstrating Respondents legal ability to enter into such agreements in other states.

Respondents must provide an explanation of how these interstate and intrastate capabilities will be achieved.

TCS Response: Comply.

TCS is uniquely suited to interconnecting with other SSPs in states other than Alabama. For example, we are currently contracted to provide ESInet and ALI professional services in the state of Tennessee, and we provide underlying ESInet functional elements in that state as well. In addition, we provide ESInet functional elements for significant parts of Florida, which may further facilitate our proposed deployment in Alabama.

To date, TCS equipment and/or services have been used to deploy approximately half of NG9-1-1 ESInets nationally; we are pleased to provide a number of example agreements and relationships, if we are selected to move forward as a result of this RFP.

3.3 TEXT TO 9-1-1 REQUIREMENTS

The intent of this section is to specify a Text solution that is in compliance with the Alliance for Telecommunications Industry Solutions (ATIS) / Telecommunication Industry Association (TIA) J STD 110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements & Architecture Specification A J STD 110 Standard.

The Board is looking for Respondents to provide a hosted solution for the processing of text-to-9-1-1 messages on Respondent’s proposed ESInet.

The Board is seeking a text to 9-1-1 emergency telecommunications system that shall possess the highest degree of resiliency, reliability, redundancy, and service availability and conforms to current and evolving industry standard.

The system shall support the delivery of 9-1-1 text calls to all participating PSAPs located throughout Alabama.

Functionally the Board's desire is to have emergency text messages (text-to-9-1-1) from all wireless carriers aggregated from Respondents' proposed solution and forwarded to the appropriate PSAP. A TCC function for all of Alabama.

Conceptually the solution will allow a subscriber to a wireless service in the U.S. to send an emergency text to 9-1-1 while in the confines of the State of Alabama and that emergency text will be sent to the appropriate PSAP for answering and processing.

Respondents proposed solution(s) shall aggregate incoming Short Message Service (SMS) text messages from the public through one interface to all Text Control Centers (TCCs) provided by wireless carriers/vendors and distribute the text message to the appropriate Public Safety Answering Point (PSAP) in the format required by that PSAP (web browser, TTY, Direct IP interface).

Respondents proposed solution(s) shall minimize interconnection points between Respondents proposed solution and the PSAP by providing a single content distribution node from the aggregator solution to the PSAP interface.

Such an interface node shall be compatible with all NENA i3 CPE, TTY, and Web-based text displays.

Respondents proposed solution(s) shall only require that a person requiring emergency assistance enter the short code '9 1 1' in their wireless device in order to have an emergency text message sent to the PSAP.

The use of any other short code to send emergency text messages is not required nor shall there be any need for a public person to register their device in order to text 9-1-1 within the defined jurisdiction.

Respondents proposed solution(s), through a distribution method, shall allow messages to be transferred between PSAPs (primary and secondary) that use a web-based browser or NENA i3 CPE interfaces.

Respondents proposed solution(s) shall provide through the distribution method the ability to provide TTY transfer of SMS texts between TTY PSAPs on the same selective router.

Respondents proposed solution(s) should provide an Aggregator function that:

- Will aggregate text-to-9-1-1 messages from multiple TCCs into a single message stream for distribution to the PSAPs
- Supports any ATIS compliant text-enabled CPE interface
- Supports transfer of text sessions between different interfaces

Respondents proposed solution(s) should provide a Distributor function that:

- Receives text-to-9-1-1 messages from the Aggregator and uses the ESRP/ECRF to route the message to the destination PSAP for the PSAPs served by the Distribution server.
- The Distributor includes:
  - TTY Interface – to handle conversion of a text message to a TTY stream for interfacing to a selective router through an Emergency Services Gateway (ESGW)
  - Web Portal – contains a portal for the web-based Respondents solution for use by the call taker

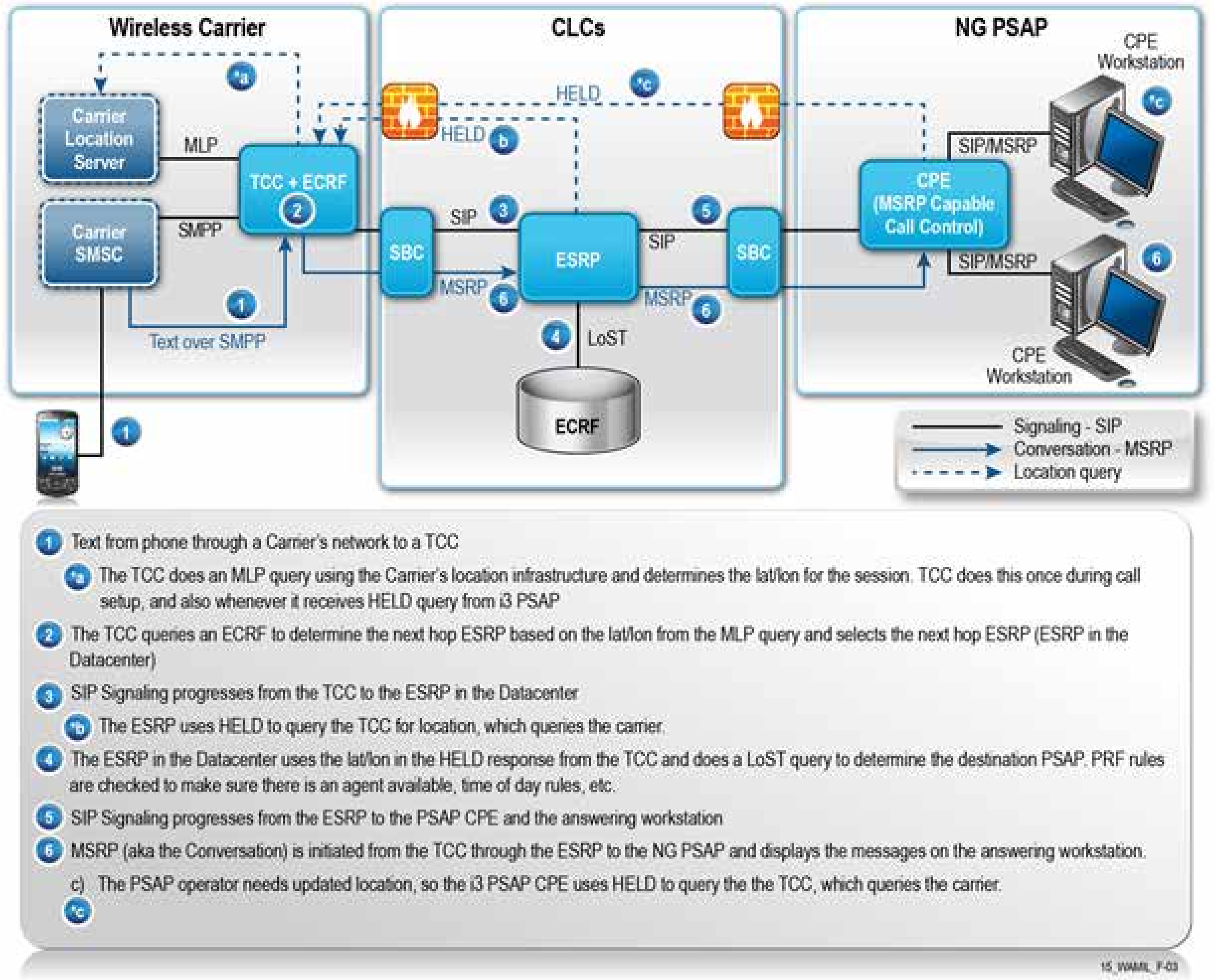
- SIP/MSRP Interface – interface between the Aggregator and the NENA i3 ESInets or MSRP CPE at the PSAP.

TCS Response: Comply.

The proposed solution complies with J-STD-110 to natively handle SIP/MSRP-based SMS-text-to-911 sessions. 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.

Exhibit 9 shows our Dallas, Texas and Raleigh, North Carolina Text Control Centers (TCCs), as TCS is a provider of TCCs to wireless carriers. This means our NG9-1-1 solution interfaces with our own TCC directly, as well as with other TCC providers. We currently 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, thereby aligning seamlessly with existing routing rules.



1 Text from phone through a Carrier's network to a TCC

*a The TCC does an MLP query using the Carrier's location infrastructure and determines the lat/lon for the session. TCC does this once during call setup, and also whenever it receives HELD query from i3 PSAP

2 The TCC queries an ECRF to determine the next hop ESRP based on the lat/lon from the MLP query and selects the next hop ESRP (ESRP in the Datacenter)

3 SIP Signaling progresses from the TCC to the ESRP in the Datacenter

*b The ESRP uses HELD to query the TCC for location, which queries the carrier.

4 The ESRP in the Datacenter uses the lat/lon in the HELD response from the TCC and does a LoST query to determine the destination PSAP. PRF rules are checked to make sure there is an agent available, time of day rules, etc.

5 SIP Signaling progresses from the ESRP to the PSAP CPE and the answering workstation

6 MSRP (aka the Conversation) is initiated from the TCC through the ESRP to the NG PSAP and displays the messages on the answering workstation.

c) The PSAP operator needs updated location, so the i3 PSAP CPE uses HELD to query the the TCC, which queries the carrier.
*c

Exhibit 9. Texting Solution Overview

3.3.1 DATA COLLECTION AND REPORTING

The proposed solution shall supply call detail record (CDR) or an equivalent for all text messages. The solution shall provide QoS information, per NENA i3 standards, for each text 'call' to ensure that SLAs are being met.

Quality of service information should be accessible through Respondents' maintenance function.

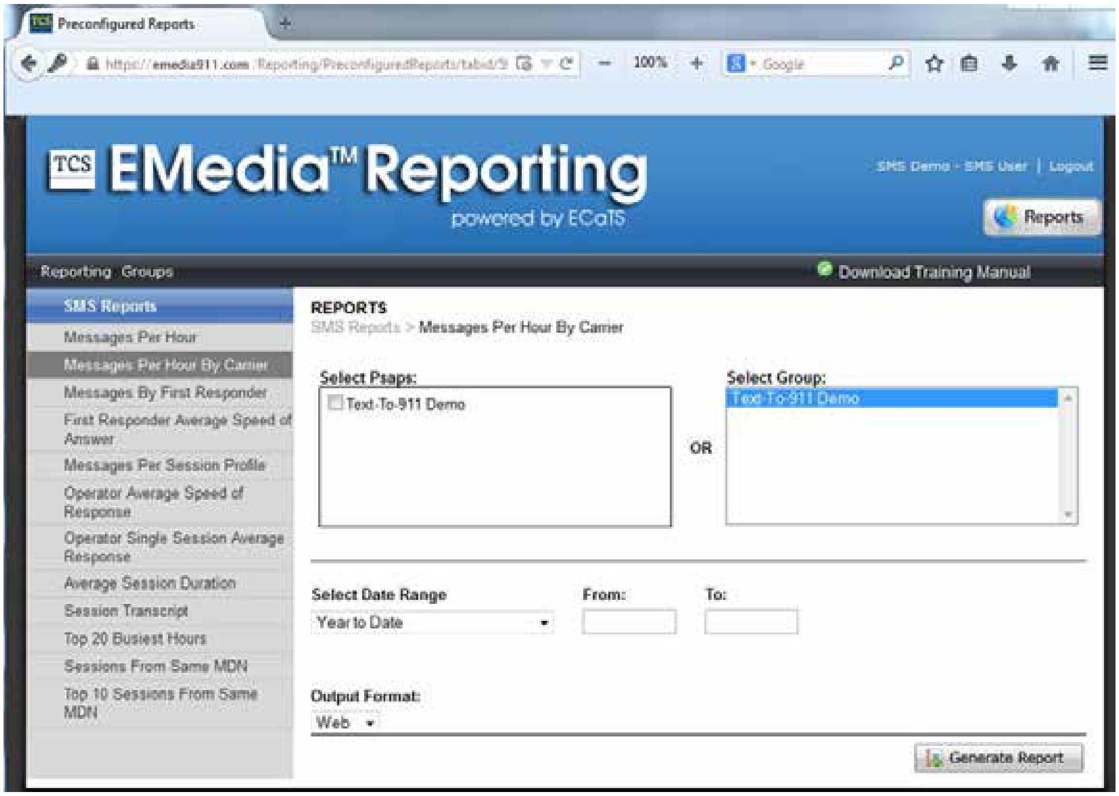
Respondents shall provide diagrams for their proposed solution showing:

- System connectivity
- System NG9-1-1 functionality including connectivity to network
- Intelligent workstation equipment

TCS Response: Comply.

TCS has partnered with Direct Technologies and their ECaTS product for text reporting. ECaTS provides full text-to-911 reporting functionality. The ECaTS Text-To-9-1-1 reporting system is a CPE-SMS agnostic reporting system and provides reporting across all PSAPs in the ECaTS system. ECaTS offers twelve standard SMS reports which provide visibility into the number of total messages sent and received, the average time to respond between caller and call taker, the tracking of top MDNs to isolate SMS abusers, and full Text-to-9-1-1 transcription, just to name a few. Similar to other ECaTS systems, these twelve standard SMS reports can be augmented with customizations that improve the overall SMS reporting value to individual PSAPs, should the standard set not fully address all reporting needs.

Exhibit 10 below shows ECaTS reporting capabilities (here as part of our EMedia platform):


Preconfigured Reports
https://emedia911.com/Reporting/PreconfiguredReports/tabid/9
100%
Google
TCS EMedia™ Reporting
powered by ECaTS
SMS Demo - SMS User | Logout
Reports
Reporting Groups
Download Training Manual
SMS Reports
Messages Per Hour
Messages Per Hour By Carrier
Messages By First Responder
First Responder Average Speed of Answer
Messages Per Session Profile
Operator Average Speed of Response
Operator Single Session Average Response
Average Session Duration
Session Transcript
Top 20 Busiest Hours
Sessions From Same MDN
Top 10 Sessions From Same MDN
Generate Report

REPORTS
SMS Reports > Messages Per Hour By Carrier

Select Psaps: □ Text-To-911 Demo

OR

Select Group: Text-To-911 Demo

Select Date Range: Year to Date
From:
To:

Output Format: Web

Exhibit 10. EMedia Reporting Screenshot

Exhibit 11 illustrates how the ECaTS solution integrates with the overall TCS solution.

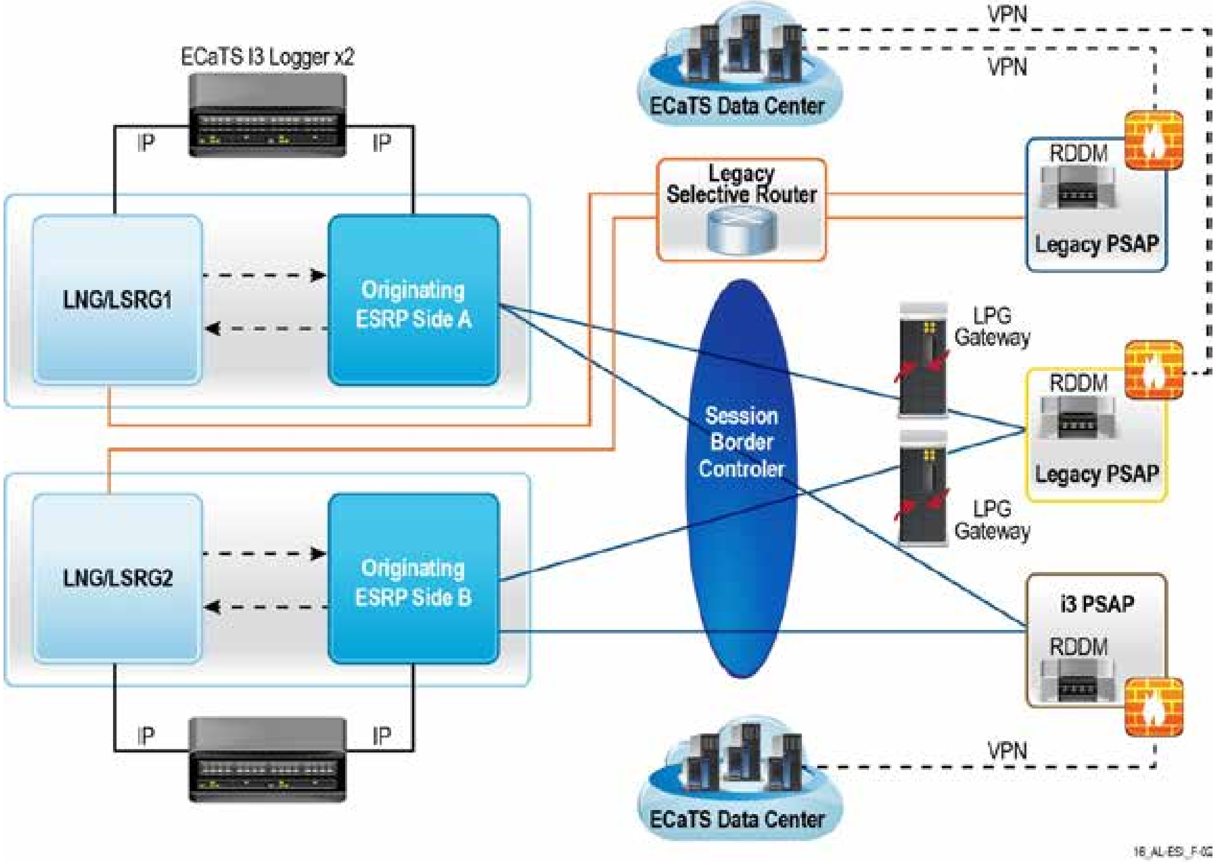


Exhibit 11. ECaTS i3 Logger

Exhibit 12 illustrates the connectivity from the ECaTS data center to an Alabama PSAP.

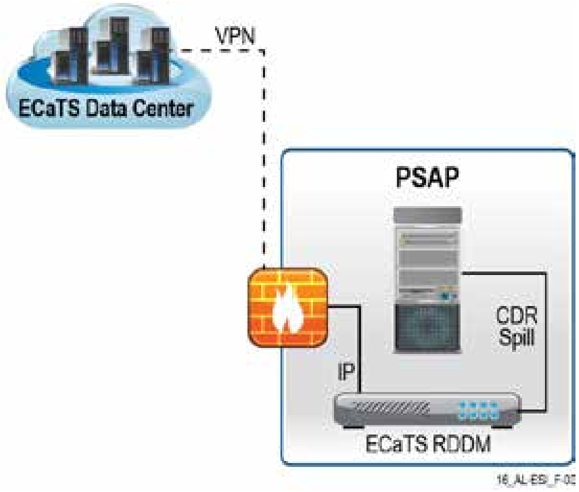


Exhibit 12. ECaTS Connectivity to PSAP

3.3.2 PSAP GRAPHICAL USER INTERFACE AND TEXT STATUS WINDOWS (BROWSER METHOD)

Respondents shall include a user interface provided for a web browser that allows a supervisor the ability to modify the system sounds and button icons.

The User interface proposed by Respondents solution must utilize Windows Graphical User Interface (GUI) interfaces using drop-down boxes, check boxes, text boxes, radio buttons. Etc. to facilitate user friendly data entry and editing.

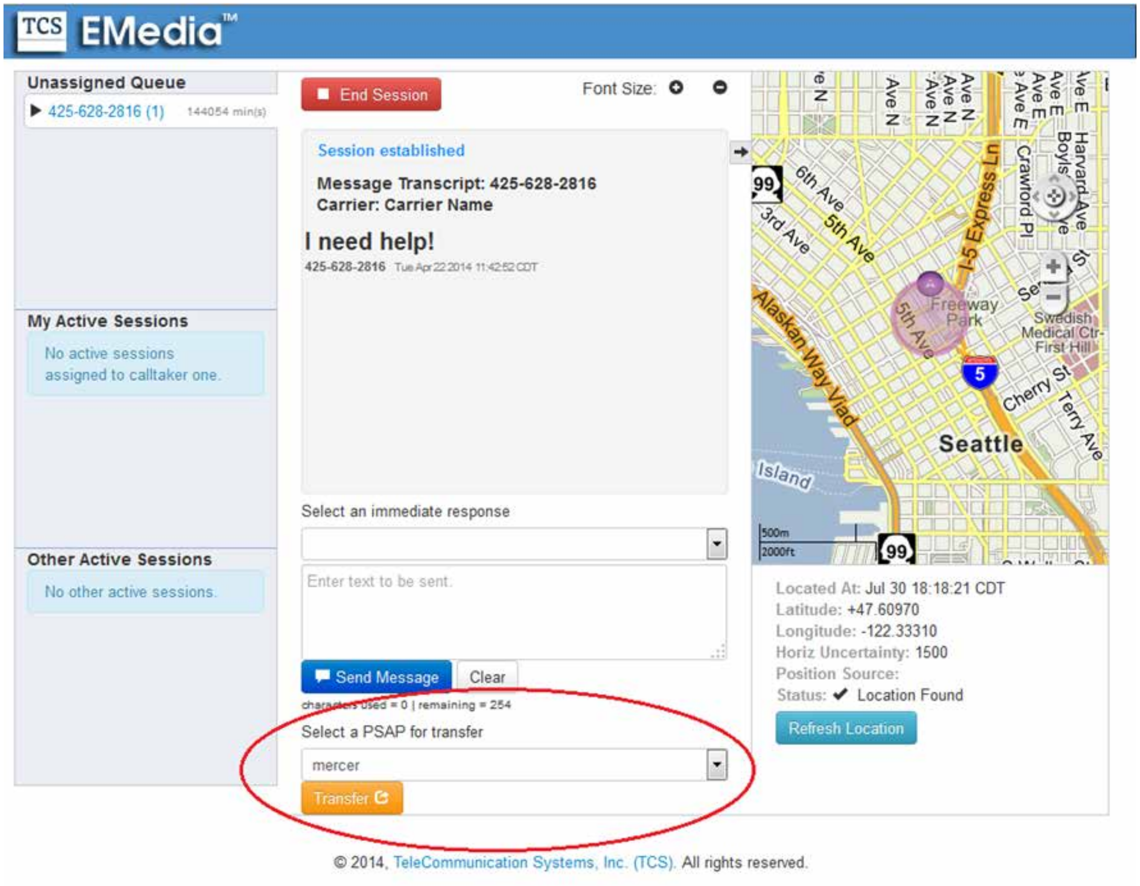
The Intelligent Workstation shall present the text-call-taker, at a minimum, with the status of the following categories:

- Number of Active Text-to-9-1-1 Calls
- Number of Text-to-9-1-1 Calls on Hold
- Number of Text-to-9-1-1 Calls ‘Ringing’
- Number of Active Text-to-9-1-1 Call takers.

TCS Response: Comply.

Our EMedia product is a secure, easy to use web GUI that enables PSAPs to interact with text-to-911 calls delivered via HTTPS. The EMedia GUI includes drop-down menus, automatic location mapping, rebid functionality, as well as assigned and unassigned queues for text-session management. An example use case involves text transfers, where a drop-down menu is used to select the destination PSAP.

Exhibit 13 below provides an example of the transfer scenario at an HTTPS web-based PSAP.



No active sessions assigned to calltaker one.

No other active sessions.

Session established

Message Transcript: 425-628-2816
Carrier: Carrier Name

I need help!
425-628-2816 Tue Apr 22 2014 11:42:52 CDT

Select an immediate response

Enter text to be sent.

characters used = 0 | remaining = 254

Select a PSAP for transfer
mercer

Located At: Jul 30 18:18:21 CDT
Latitude: +47.60970
Longitude: -122.33310
Horiz Uncertainty: 1500
Position Source:
Status: ✓ Location Found

© 2014, TeleCommunication Systems, Inc. (TCS). All rights reserved.

Exhibit 13. Transfer Capability

The EMedia product enables PSAP administrators to create a list of destination PSAPs to be enabled for transfers on the HTTPS web portal via the PSAP admin GUI. As a result, the PSAP has complete control over the transfer function and can make decisions based upon jurisdictional preferences.

Our EMedia service gives aggregates all text-to-911 traffic from multiple wireless carriers and text control center (TCC) into a single transitional web interface to the PSAP legacy teletypewriter (TTY) connection to the selective router. The EMedia architecture offers a common interface to the PSAP, regardless of the number of wireless carriers or TCC vendors. EMedia is built entirely using NENA i3-compliant elements adapted for use by nonvoice media. It is also fully compliant with Alliance for Telecommunications Industry Solutions (ATIS)/JSTD-110 standard text delivery methods.

High-level EMedia features:

- Aggregates the text-to-911 traffic from multiple wireless carriers and TCC vendors.
- Provides a consistent user experience via a single web interface.
- Establishes a single legacy TTY interface to the selective router.
- Complies fully with NENA i3 and ATIS/JSTD-110 standards.

Exhibit 14 describes the network components and its supported interfaces.

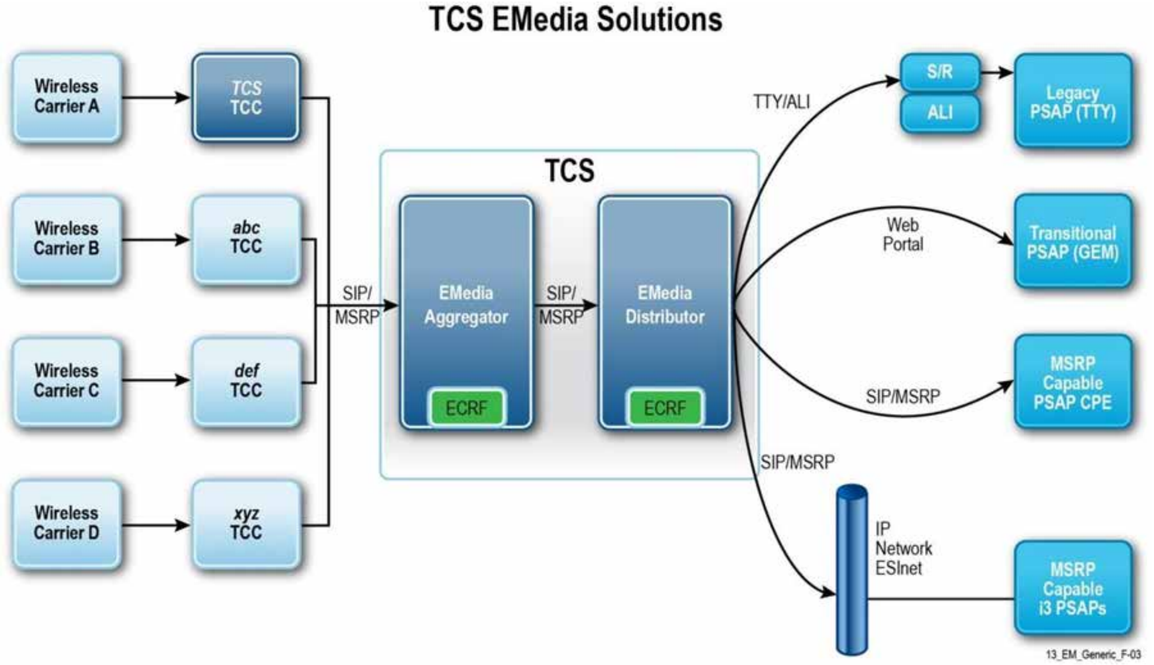


Exhibit 14. TCS EMedia Solutions

TCS provides the following components as part of EMedia:

- **EMedia Aggregator—**Aggregates text-to-911 messages from multiple TCCs into a single message stream. The EMedia Aggregator uses an ESRP/ECRF to route the message to the destination EMedia Distributor. There can be many deployments of the EMedia Distributor. The chosen EMedia Distributor uses an ESRP/ECRF to select the final route to the destination PSAP or ESInet.
- **EMedia Distributor—**Receives text-to-911 messages from the EMedia Aggregator and uses an ESRP/ECRF to route the message to the destination PSAP for those PSAPs the EMedia Distributor serves. Acts as a contained SMS-text-to-9-1-1, i3-based NG9-1-1 system.

The EMedia system includes the following functions:

- **HELD Interface—**The interface for the conveyance of location information.
- **Web Portal—**A web GUI that allows text call takers to receive and respond to text-to-911 messages as well as transfer text sessions to other PSAPs.
- **SIP/MSRP Interface—**The interface between the EMedia Aggregator on one side and NENA i3-based ESInets or MSRP-based CPEs on the other.
- **ALI Link—**The dynamic ALI, where caller location data is stored. This data is accessed in the same way as is a wireless caller's location.

SECTION 4 ANGEN i3/NG CORE SERVICES REQUIREMENTS

4.1 NENA I3 NG CORE FUNCTIONAL REQUIREMENTS

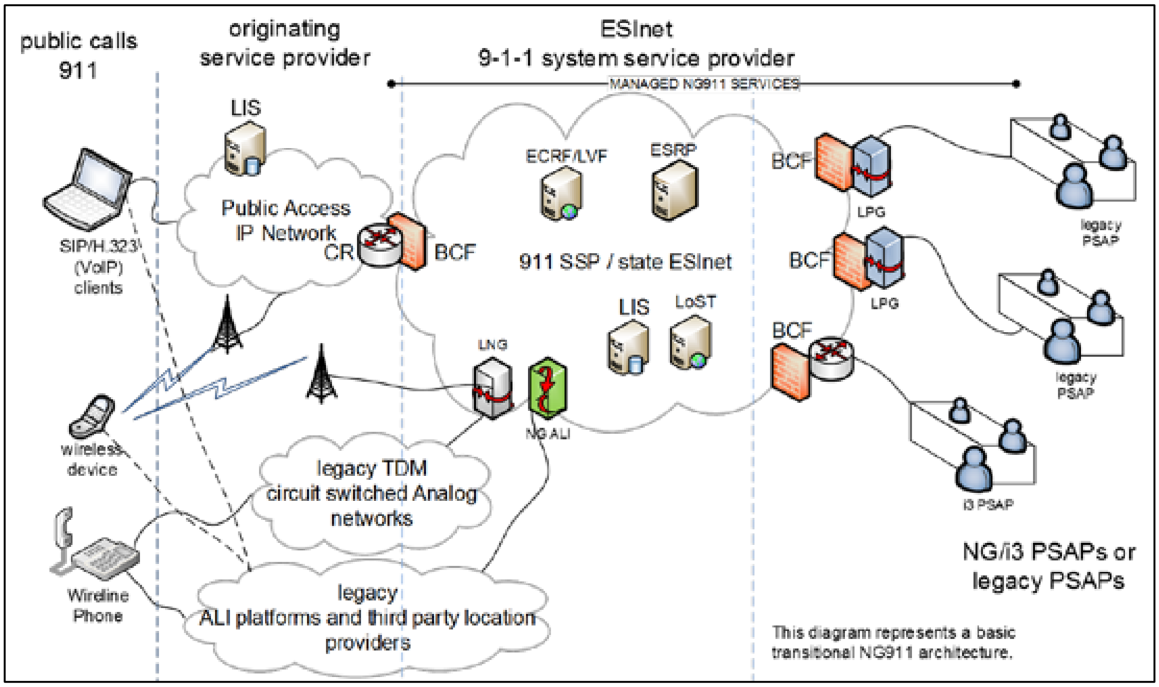

public calls 911
originating service provider
ESInet 9-1-1 system service provider
MANAGED NG911 SERVICES
LIS
Public Access IP Network
CR
BCF
SIP/H.323 (VoIP) clients
ECRF/LVF
ESRP
911 SSP / state ESInet
LIS
LoST
LNG
NG ALI
BCF
LPG
BCF
LPG
BCF
legacy PSAP
legacy PSAP
i3 PSAP
wireless device
Wireline Phone
legacy TDM circuit switched Analog networks
legacy ALI platforms and third party location providers
NG/i3 PSAPs or legacy PSAPs
This diagram represents a basic transitional NG911 architecture.

Figure 8 - ANGEN Conceptual Design Diagram

The proposed system shall be designed to meet and expand the current capabilities of the ANGEN system and be scalable and adaptable to accept new payloads (such as Text, Pictures and Video) that may be directed by the Board for deployment during the term of the contract.

ANGEN is currently configured as a wireless carrier aggregation point, which is interconnected to every S/R in Alabama, which then serve and deliver wireless 9-1-1 calls to the PSAPs in AL.

The proposed system is required to provide or accommodate NG9-1-1 core functional elements as well as legacy transitional elements for the continued and future operation of ANGEN.

Those NG9-1-1 core functional and legacy transitional elements include:

- Border control function (BCF)
- Emergency call routing function (ECRF)
- Emergency services routing proxy (ESRP)
- Legacy network gateway (LNG)
- Legacy PSAP gateway (LPG)
- Legacy Selective Router Gateway (LSRG)
- Location Validation Function (LVF)
- Policy routing function (PRF)

Respondents shall explain where these functional components are physically located in their proposed solution and describe how they will operate.

It is recognized that all of the functions may not be required at this time and that some may only be added after transition or at some future point as technologies or standards evolve.

Suggested components that are not used or are not needed in the Respondents proposed solution must be clearly noted as an exception; and an explanation must be given for eliminating the particular component to perform the ANGEN capability.

TCS Response: Comply.

We propose our Intrepid9-1-1 Next Generation Core Services (NGCS) with options for GeoComm's LVF, and Intrepid9-1-1 LPG services. Exhibit 15 summarizes the TCS Intrepid9-1-1 product family, with the GeoComm options.

Exhibit 15. Intrepid9-1-1 Solution Components

Product Group	Product Elements
Intrepid9-1-1 Next Generation Core Services	▪ Intrepid9-1-1 ESRP ▪ Intrepid9-1-1 PRF ▪ Intrepid9-1-1 LNG/LSRG ▪ Intrepid9-1-1 BCF
Intrepid9-1-1 Options	▪ Intrepid9-1-1 ECRF ▪ GeoComm LVF ▪ GeoComm Managed GIS Services ▪ Intrepid9-1-1 LPG
Standalone Option	▪ Intrepid9-1-1 ALI

4.2 BORDER CONTROL FUNCTION (BCF)

Per the NENA i3 NG9-1-1 specification, the network must be configured with a Border Control Function (BCF) at all ingress and egress points.

The BCF shall support a variety of direct IP interconnection arrangements between the ESInet and external IP networks depending on the level of mutual trust that exists between the respective networks.

It is strongly recommended that BCF's are located at a minimum of two geographically diverse points of interconnection (POI), and support 99.999% availability interconnections to external networks.

Respondents shall explain the features and capabilities of their proposed BCF, along with a brief explanation of how high availability will be achieved.

TCS Response: Comply.

TCS will secure entry into the ESInet as required—on both ingress and egress sides of the network—with redundant network appliances. The proposed solution includes two Internet firewalls at each PSAP to provide TCS remote support and connection to the ESInet.

The BCF is made up of two elements: a firewall, and a session border controller (SBC).

In an ESInet, the SBC applies control over SIP signaling and associated media to ensure the call and call characteristics presented to the ESInet are predictable and acceptable. All calls are expected to pass through the SBC, in particular those that originate from an unmanaged source.

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 requirement; these include Cisco, Dialogic, Acme Packet, and Sonus.

The SBC will support the following features that align with generally accepted security practices:

- Depending on the deployment model, the SBC either acts as a firewall or works cooperatively with an existing firewall
- It acts as a transcoder for codec conversion
- It helps resolve any topology issues that stem from either network address translation (NAT) deployment or bandwidth misalignments; for example, it prevents low-speed links from being oversubscribed with voice traffic

With regard to SIP repair, the SBC attempts 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 to no impact on general call delivery and bandwidth performance characteristics, as it is a high-performance, hardware-based component.

The firewall component of the BCF employs all the characteristics normally found in a typical firewall application, including the following elements specific to NG9-1-1 applications:

- Support for TLS for those originating call entities that request TLS connections
- Port firewalling—Permission for traffic is allowed only through certain ports opened in the firewall
- Pinhole firewalling—Ports are opened to support calls on an individual basis, based upon the requested media port (RTP); once the call is completed, the port is closed again
- Stateful packet inspection
- Deep-packet scanning—The firewall works in conjunction with other firewalls that provide the BCF for ESInets in a common manner so that an attack on one firewall is known by all

4.3 EMERGENCY CALL ROUTING FUNCTION (ECRF)

Respondents shall include an emergency call routing function (ECRF) in their proposed solution that utilizes geographic location information to route emergency calls to the appropriate PSAP.

The ECRF shall be designed according to NENA08-003 standards and be implemented using diverse, reliable and secure IP connections.

Respondents shall supply an ECRF function that meets a minimum of 99.999% availability

Respondents providing an ECRF must ensure that it is accessible from outside the ESInet and that the ECRF permits querying by an IP client/endpoint, a Legacy Network Gateway (LNG), an Emergency Services Routing Proxy (ESRP) in a next generation Emergency Services network, or by some combination of these functions.

An ECRF accessible inside an ESInet must permit querying from any entity inside the ESInet. ECRFs provided by other entities may have their own policies on who may query them.

An origination network may use an ECRF, or a similar function within its own network, to determine an appropriate route, equivalent to what would be determined by the authoritative ECRF, to the correct ESInet for the emergency call. Respondents shall describe the functionality of such an ECRF equivalent and document where this functional element resides within their proposed solution.

The ECRF shall support a routing query interface that can be used by an endpoint, ESRP, or PSAP to request location-based routing information from the ECRF. Additionally, it must support both iterative and recursive queries to external ECRF sources.

The ECRF must interface with the Location to Service Translation (LoST) protocol (RFC5222) and support LoST queries via the ESRP, PSAP customer premise equipment (CPE), or any other permitted IP host.

The proposed ECRF must allow for rate limiting queries from sources other than the proposed ESRP(s), and provide logging of all connections, connection attempts, and LoST transactions.

The ECRF must be designed and implemented to support the ability for GIS data management functions to ensure accurate location data is maintained.

The ECRF must support:

- Location error correction.
- Routing of calls based on geographical coordinates and civic addresses.
- Utilize common GIS boundaries (to include but not limited to Municipal, Police, Fire, EMS).
- Permit LoST association with each layer.
- Comply with NENA 02-010 and NENA 02-014.
- Must support dynamic updates to GIS without disruption of the ECRF.
- Validation of GIS updates before they are applied.

GIS is handled locally throughout the State of Alabama. Respondents shall define their method for collecting local PSAP related GIS information and establishing the ECRF.

Respondents shall explain where the ECRF will be located and how it will operate within their proposed solution.

Respondents shall describe how the proposed ECRF and its capabilities, features, functions and protocols provides high reliability routing for all 9-1-1 call types.

Respondents shall describe the interface to the system that provides the ability to upload location information once the Extensible Markup Language (XML) is published and approved for general use, as determined by the Board.

TCS Response: Comply.

ECRF

TCS has included its Intrepid9-1-1 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 Alabama's GIS system. Attributes provided must meet the minimum Intrepid9-1-1 ECRF specifications, which we will determine with input of Alabama's GIS personnel.

The application server supporting the function is a redundant array of Windows servers running Esri ArcGIS and TCS ECRF software. 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:

- Point data
- Circles
- Arc bands
- Polygons

In addition, the ECRF is capable of handling many service boundaries that represent the downstream ESInet/PSAP boundaries and is capable of the following output responses:

FindService

- GetServiceBoundary
- ListServicesByLocation

Alabama GIS data will be loaded onto each ECRF server as part of the equipment staging process. Connectivity to an ArcSDE replica copy of the GIS master database eliminates the prospect of a single point of failure.

Intrepid9-1-1 ECRF has built-in audits that will notify Alabama systems administrators when data received from the single GIS master database does not meet conformity requirements. Alabama and TCS will work directly with the appropriate 9-1-1 entities to make any necessary updates to GIS data. Alabama will then resynchronize updated GIS data to the TCS "auditing" geodatabase via the Spatial Information Function (SIF). If data has not passed audit, the workflow described above must be repeated until such data issues have been remedied by the State.

The ECRF/LVF GIS databases will be automatically synchronized at regular intervals with the master GIS database via either Open Geospatial Consortium (OGC) Web Feature Service (WFS) GIS replication or Esri spatial database engine (SDE) geodatabase replication.

GIS Data Management

With our dedicated partner and their experienced project team, GeoComm will provide the state of Alabama with an initial NG9-1-1 GIS dataset for routing calls, based on existing data available within the state and from individual ECD's. This will include mechanisms for continually updating the dataset to produce seamless, statewide coverage. GeoComm's solution is complete with 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, GeoComm's NG9-1-1 GIS managed services solution includes the following elements:

- Subscription-based access to GeoComm's enterprise GIS data management tools:
  - GeoLynx Server GIS Portal for easily transferring GIS data and viewing GIS update status
  - GeoLynx DMS 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 quality control plan, and identify key roles in the NG9-1-1 GIS data workflow process
- NG9-1-1 GIS Managed Services providing on-going GIS data transformation, aggregation, QA/QC and reporting

Throughout this project, GeoComm will dedicate time to project management and ongoing communication. By partnering with GeoComm you will know the status of your project, that deliverables are being met, and have confidence your objectives are being carried through. GeoComm will provide regular status updates that will include:

- General progress updates
- Meetings held, planned, or needed
- Issues/problems encountered or anticipated
- Goals for the next reporting period
- Schedule review
- Customer responsibilities

The TCS team 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 onsite at a centrally located meeting space. The agenda will additionally include reviewing project objectives and goals, defining mutual expectations, and establishing communication processes.

Statewide GIS Data Aggregation

GeoComm will create an initial statewide GIS dataset for NG9-1-1 by combining GIS data layers from the state and local entities, including data all of ECD's that have 9-1-1 GIS data. GeoComm's method of local data submission from individual counties or regional authorities is through the GeoLynx Server GIS Portal or FTP. Each local entity must provide agency jurisdiction copies of their MSAG and ALI databases.

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
- PSAP Routing Boundary

If not available from the state, individual counties, or regional authorities, GeoComm can populate the street/road centerline and county boundary layers based upon publically-available sources (such as U.S. Census Bureau's TIGER/Line shapefiles). If not available, GeoComm can develop PSAP and/or 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 ECD and GeoComm.

Note: While GeoComm will provide ongoing QA/QC audits and the ECRF will not accept data updates that fail quality control checks, the quality of the data included in the statewide dataset is ultimately the responsibility of individual ECD's.

Additional GIS layers, such as site/structure address points, can be added as they are available from ECD's

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. As available, the individual GIS data layers will then be merged into a statewide dataset. In order to create topological accuracy across county boundaries, GeoComm will also create reference layers along ECD boundaries to which local authorities can match roads and allow for vehicle routing across ECD lines. A seamless polygon layer representing all ECD's in the state will need to be provided by the state of Alabama in order for this additional reference layer to be created.

After layers are aggregated together, the GIS dataset will be loaded into the GeoLynx Server GIS Portal. As part of this process, GeoComm will:

- Create, configure, and load Esri address locators for simple address lookups
- Design Esri ArcGIS map documents (.mxd) for GeoLynx Server (layers, layer order, layer visibility, scale dependent display, symbology, labeling, etc.) based on project stakeholders' preferences
- Develop, configure, test, and publish ArcGIS Server 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.

After the ECRF has been implemented, GeoComm will update the statewide GIS dataset based on updates sent by ECD's up to twice monthly prior to the acceptance of the ESInet. After the state has accepted the ESInet and the NG9-1-1 system has been implemented, GeoComm will provision GIS updates to the ECRF on an up-to-daily basis, as described in Section 6.8.

The statewide GIS dataset and GeoLynx Server GIS Portal will be hosted in a secure data center, described in more detail in section 4.10:

GIS NG9-1-1 Data Model Development

GeoComm will work with the state to develop a GIS data model which will be used as a guide in the development and enhancement of key GIS layers for Alabama's NG9-1-1 system. GeoComm will work with the state to review resources which will influence the final design of the data model. Resources and workflows to consider include:

- General progress updates
- Dispatch mapping system requirements
- NENA standards
- ECD resources that contribute to the address information
- ECD public safety maintenance procedures:
- ALI management
- MSAG maintenance
- ECD GIS workflows
- Maintenance software data requirements
- Workflows defined by the maintenance software

The GIS data model will be used for the aggregation of an initial statewide GIS dataset as well as for the ongoing maintenance and further enhancement of GIS data, as described in Section 6.8. The data model will clearly outline the feature data sets, feature classes, and domains specific to Alabama's NG9-1-1 needs.

GeoComm understands the data model must fit the needs of the dispatch mapping system standards, NENA standards, and allow for future development of attributes. GeoComm has across-the-board knowledge of data models, addressing, MSAG and ALI database development, GPS data collection, and digital base map development. Our experience will enable the creation of a solid data model for the state of Alabama.

Note: 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.

Ongoing GIS Data Maintenance

GeoComm will work with the State to establish a mutually-agreeable schedule for GIS data maintenance updates and provisioning, including a deadline for local authorities to submit GIS changes for processing. Once the state's NG9-1-1 system has been implemented, data submitted before a daily deadline will undergo quality control validation checks and be processed by the following day's deadline for provisioning to the ECRF, excluding holidays and weekends; datasets that pass validation checks will be provisioned into 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.

To establish this process, GeoComm will work with the state and local stakeholders to establish a maintenance workflow. Once the initial statewide database has been created, GeoComm will provide GIS managed services to ensure the statewide database is continually updated with improved data submitted by local authorities. GeoComm will additionally work with the state to establish a process for time-critical or time-sensitive updates that are needed during weekends or holidays, such as jurisdictional boundary changes that go into effect on a weekend or holiday.

Note: If incoming GIS data is submitted using a field structure different from what was previously submitted and accepted, it cannot be processed without revising the extract-transform-load (ETL) process. A GeoComm specialist will work with the submitting ECD on the next business day to edit the ETL process so that the new field structure can be incorporated into the system.

Maintenance Workflow Development

During the same trip as the project initiation meeting, GeoComm 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.

GeoComm’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 Alabama
- 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 to be consistently processed according to a mutually-agreeable daily submission and provisioning deadline, excluding holidays and weekends.

GeoComm 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, GeoComm 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 Emergency Call Routing Function/Location Validation Function (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). 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 will also provide a train-the-trainer training session focusing on how to incorporate GeoComm's GIS Data Management tools into the new maintenance workflows. Training curriculum includes:

- Core GeoLynx Server tool functionality
- GIS data request management
- Downloading GIS data from the GIS Portal
- GeoLynx DMS Discrepancy Viewer functionality
- Accessing QA/QC reports via GIS Portal or GeoLynx DMS 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.

Ongoing Quality Control/Quality Assurance

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.

GeoComm will implement a QA/QC process to ensure data meets the state of Alabama's NG9-1-1 criteria; this process will automatically report GIS errors to the authoritative 9-1-1 source for correction. 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.

The QA/QC plan will be discussed during the project initiation and GIS data management collaboration meetings. A GeoComm GIS Project Manager will collaborate with project stakeholders to develop a formal QA/QC plan. The quality control approach, including regular communication of QA/QC results to local GIS entities, will be documented. The plan will also detail initial on-going quality control processes to be performed on local GIS data submitted to GeoComm for provisioning into the ECRF. 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 quality control processes are performed prior to coalescing the updates into the statewide GIS dataset to ensure proper topology and data integrity. These processes may include the actions listed in Exhibit 16.

Exhibit 16. Topology Quality Control

Topology Aspect	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 quality control. These reports will be transmitted to the sending agency and, optionally, to stakeholders at the state level for performance monitoring.

MSAG/ALI Synchronization

As the state transitions to the full implementation an NG9-1-1 system that uses GIS data to route incoming calls, it is important that the GIS data contain the information located within each ECD's MSAG and ALI database. GeoComm will thus produce annual audits of each ECD's GIS data in comparison to its MSAG and ALI database.

First, GeoComm 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, GeoComm 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 will also 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 ECDs 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.

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, GeoComm 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 provisioned into the ECRF. This solution includes:

- Access to GeoComm enterprise GIS data management tools:
    - GeoLynx Server GIS Portal for transferring GIS data, viewing GIS update status and downloading QA/QC results
    - GeoLynx DMS Discrepancy Viewer to communicate GIS data errors to source GIS agencies for resolution
- GIS data normalization, QA/QC, and error reporting according to a mutually-agreeable daily schedule, excluding holidays and weekends.

Note: The GeoLynx Server GIS Portal will be hosted in a secure datacenter, described more in section 4.10, and provided to project stakeholders as a service.

A GeoComm Project Manager will visit the state at a central location on an annual basis for a one-day meeting. The goal of this annual meeting will be to review progress made in the previous year and ensure the state's GIS data is meeting the state's maintenance goals.

4.4 EMERGENCY SERVICES ROUTING PROXY (ESRP)

The proposed solution must include an emergency service routing proxy for call delivery to the appropriate PSAP based upon location and routing rules.

Respondents shall explain where the ESRP will be located and how it will operate within their proposed solution.

This includes Carrier to ESRP, ESRP to ERSP and ESRP to call-taker routing.

Respondents shall configure the ESRP according to NENA 08-003 specifications and describe the ability of the ESRP to route SIP messages to a call taker.

Respondents shall explain how the ESRP interfaces to the ECRF and to the PRF to ensure that routing instructions, routing policies and possible event notifications that alter call routing scenarios are acknowledged.

Per NENA 08-003 for typical 9-1-1 calls received by an ESRP it;

1. Evaluates a policy “rule set” for the queue the call arrives on

2. Queries the location-based routing function (ECRF) with the location included with the call to determine the "normal" next hop (smaller political or network subdivision, PSAP or call taker group) URI.

3. Evaluate a policy rule set for that URI using other inputs available to it such as headers in the SIP message, time of day, PSAP state, etc.

The result of the policy rule evaluation is a Uniform Resource Identifier (URI). The ESRP forwards the call to the URI.

The ESRP shall support SIP SUBSCRIBE/NOTIFY in order to understand the status of both upstream and downstream elements.

Respondents shall describe their proposed ESRP solution.

TCS Response: Comply.

Intrepid9-1-1 ESRP/PRF does not currently support SIP SUBSCRIBE/NOTIFY to update the state of a PSAP. This feature is on the TCS development roadmap, but will be completed in time for deployment.

The proposed Intrepid9-1-1 ESRP/PRF is an i3-compliant ESRP soft switch employed to facilitate call routing on behalf of a calling endpoint, whether that endpoint is a legacy or next generation (SIP) one. The ESRP and PRF are responsible for coordinating call routing via ECRF/LoST queries. Intrepid9-1-1 is also responsible for policy implementation for NG9-1-1 applications and is the replacement for legacy Selective Routing (SR) technology. It includes a web-based LoST service that fulfills requests to map a call location. Details regarding the ESRP and PRF interaction are listed in the following section.

4.4.1 POLICY ROUTING FUNCTION (PRF)

The Policy Routing Function (PRF) is the primary routing component of the ESRP. The ESRP uses defined routing policies within the ESInet and the NENA i3 network to deliver calls to the call-takers.

The PRF function requires the ability of the ESRP to assist in dynamically routing and re-routing calls based upon other rules beyond normal operation.

Respondents shall describe how they will operate the PRF functionality and explain how they will implement a proxy that is customizable based upon rules set by threshold or by manual intervention.

Additionally, Respondents shall describe what user interface will be used to modify policy rules and what i3 functions can affect policy changes for call routing.

TCS Response: Comply.

Emergency Services Routing Proxy with Policy Routing Function

The ESRP and PRF are interrelated, based upon the need for the ESRP to verify the PSAP state in the PRF so as to determine the default route. As a result, TCS references both functional elements combined as an ESRP/PRF. The ESRP/PRF will be housed in the CLCs. The ESRP is the base routing function for all emergency calls for NENA i3-compliant NG9-1-1 systems. The function of the ESRP is to route a call to the next hop. TCS configures the ESRP to support queued calls.

PRF Policies Database Capabilities

TCS provides an ESRP/PRF to supply final policies before completing the call. In compliance with NENA standards and subject to the state of Alabama’s approval, our NG9-1-1 system—via the PRF—will assign alternate and overflow routing policies as well as offer PSAPs a web service portal with the capability to define and set their PSAP state.

PSAP State Settings

TCS will use a NENA i3-compliant PRF that allows Alabama's member PSAPs to define different types of routing policies. TCS can configure the PRF to close a PSAP for certain hours or days of the week, on holidays, or during any scheduled time period. This call metering feature can be adjusted to accommodate reduced staffing, PSAP equipment malfunctions, or any other event that affects a PSAP's availability.

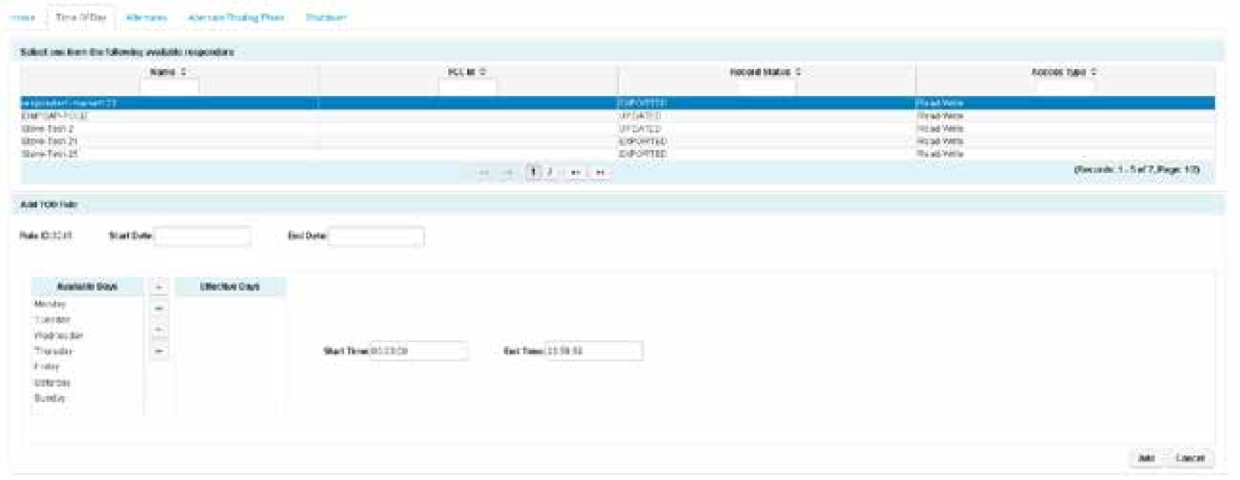
PRF Invalid Rules

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 that are invoked in the event a specified PSAP set is not available. These measures generate Simple Network Management Protocol (SNMP) traps gathered and analyzed by the TCS NOC staff.

PRF Web Access

Intrepid9-1-1 provides a web-based portal for managing PRF rules. These rules are validated to prevent routing errors; once their intent is confirmed, the transaction is completed and logged. Screenshots of some sample events are shown in the following exhibits.

Exhibit 17 shows a user adding a Time of Day rule.



Select one from the following available responders

Name	PCL Id	Record Status	Access Type
[illegible]		EXPORTED	Read Write
EMPSAP-PCL12		UPDATED	Read Write
Store-Tech 2		UPDATED	Read Write
Store-Tech 21		EXPORTED	Read Write
Store-Tech-25		EXPORTED	Read Write

(Records: 1 - 5 of 7, Page: 1/2)

Add TOD Rule

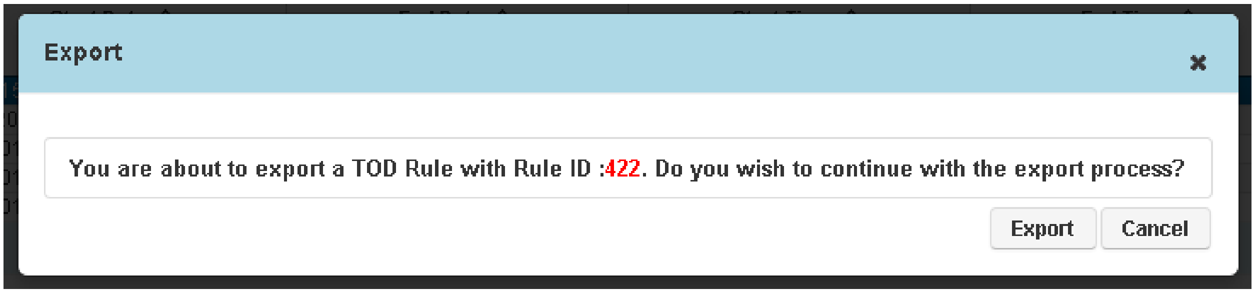
Rule ID:3215 Start Date: End Date:

Available Days	Effective Days
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	
Saturday	
Sunday	

Start Time: 00:23:00 End Time: 23:59:59

Exhibit 17. Intrepid9-1-1 User Adds Time of Day Rule.

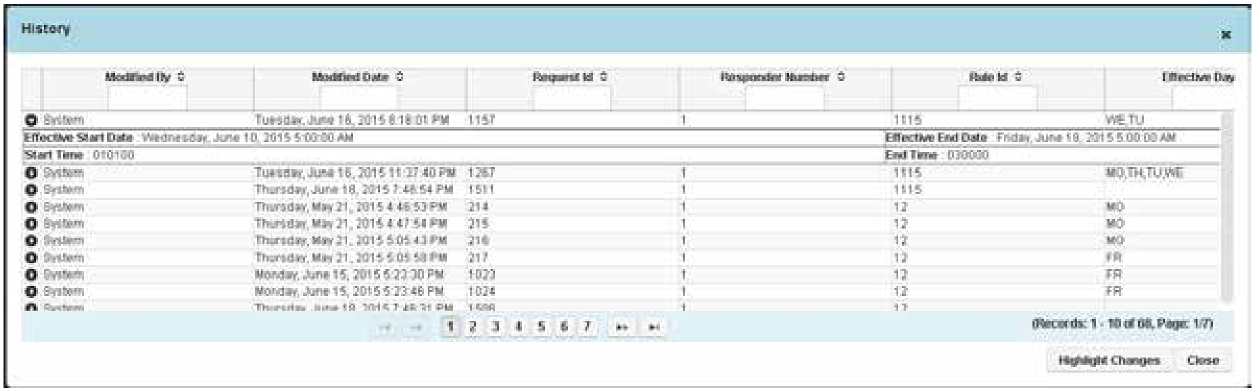
Exhibit 18 shows a confirmation screen for the user.


Export

You are about to export a TOD Rule with Rule ID :422. Do you wish to continue with the export process?

Exhibit 18. Intrepid9-1-1 Confirmation Screen

Exhibit 19 shows a summary view of transaction logs. Additional details regarding 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 8:18:01 PM	1157	1	1115	WE,TU
Effective Start Date : Wednesday, June 10, 2015 5:00:00 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	1267	1	1115	MO,TH,TU,WE
System	Thursday, June 18, 2015 7:48:54 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 5:05:58 PM	217	1	12	FR
System	Monday, June 15, 2015 5:23:30 PM	1023	1	12	FR
System	Monday, June 15, 2015 5:23:46 PM	1024	1	12	FR
System	Thursday, June 18, 2015 7:46:31 PM	1508	1	12	

(Records: 1 - 10 of 68, Page: 1/7)

Exhibit 19. Intrepid9-1-1 Summary View of Transaction Logs

4.5 LEGACY NETWORK GATEWAY (LNG)

The LNG logically resides between the originating network and the ESInet and allows i3 enabled PSAPs to receive emergency calls from legacy originating networks.

Calls originating in legacy wireline or wireless networks must undergo signaling interworking to convert the incoming Multi-Frequency (MF) or Signaling System Number 7 (SS7) signaling to the IP-based signaling supported by the ESInet.

Thus, the LNG supports a physical SS7 or MF interface on the side of the originating network, and an IP interface which produces SIP signaling towards the ESInet, and must provide the protocol interworking functionality from the SS7 or MF signaling that it receives from the legacy originating network to the SIP signaling used in the ESInet.

The LNG shall be implemented for routing emergency calls to the appropriate ESRP in the ESInet.

To support this routing, the LNG must apply specific interwork functionality to legacy emergency calls that will allow the information provided in the call setup signaling by the wireline switch or MSC (e.g., calling number/ANI, ESRK, cell site/sector represented by an ESRD) to be used as input to the retrieval of location information from an associated location server/database.

The LNG shall use this location information to query an ECRF and obtain routing information in the form of a URI.

The LNG must then forward the call/session request to an ESRP in the ESInet, using the URI provided by the ECRF, and include callback and location information in the outgoing signaling.

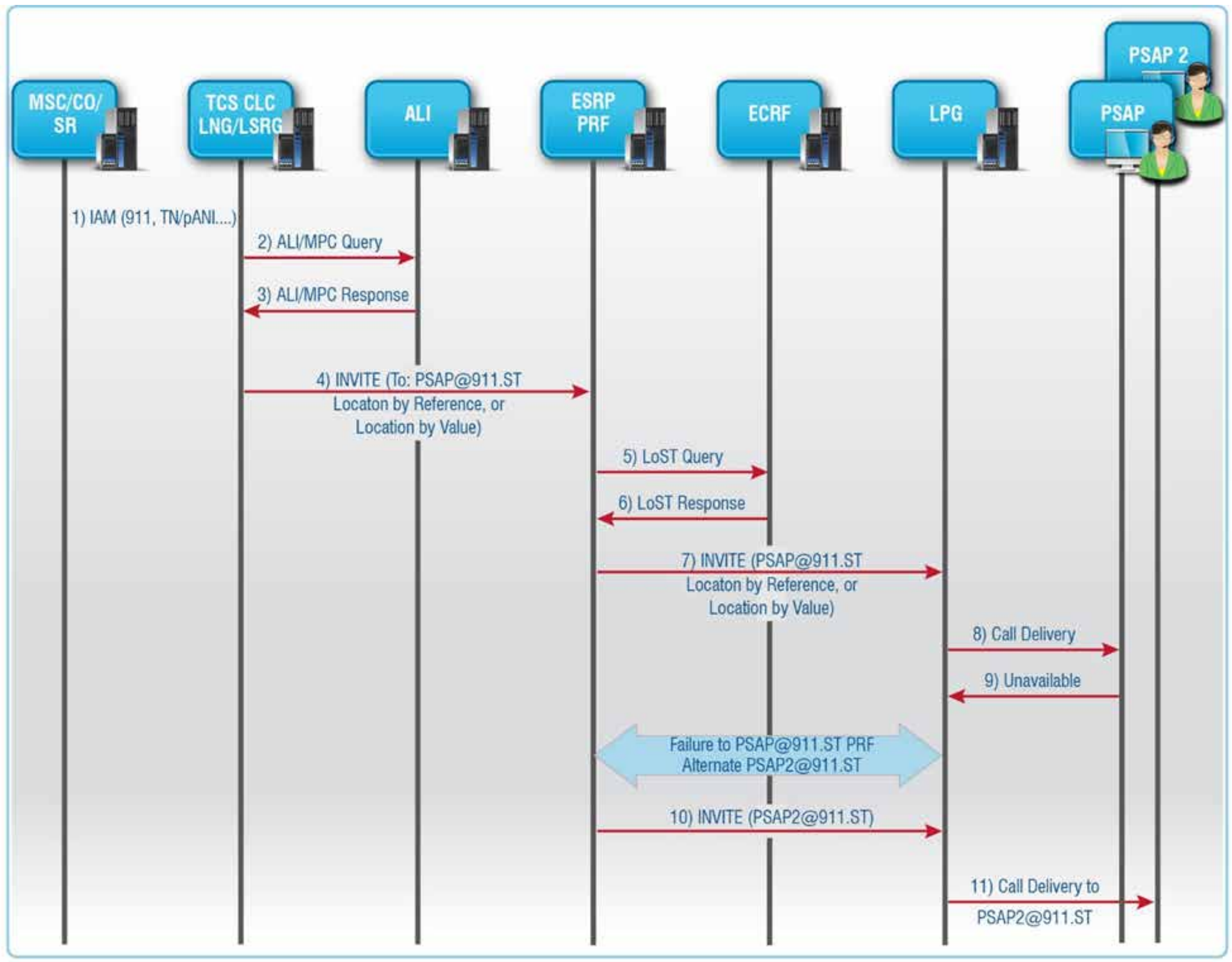
While in operation LNG shall be capable of appending supplemental and supportive call information such as location and callback number to the call prior to the ESInet.

The LNG shall also be capable of supporting SIP SUBSCRIBE/NOTIFY in order to understand any downstream elements status and then implement policy routing should a nominal route for a call not be available.

Respondents shall describe how their proposed solution permits a legacy network gateway (LNG) function to integrate the legacy network with the ANGEN core.

TCS Response: Comply.

To deliver the required interworking with legacy systems, the TCS solution provides LNG and LSRG. The LNG/LSRG is further divided between the Protocol Interwork Function (PIF), located locally, and the 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 shown in Exhibit 20.



15_WAMIL_F-07

Exhibit 20. Call Flow Diagram

The proposed Intrepid9-1-1 LNG provides location by value (LbyV), populating the PIDF-LO within the SIP messaging with the full location of the caller via interaction with whatever legacy ALI database management system (DBMS) infrastructure may exist or be implemented. This interaction complies with the NENA i3 standard. Also, Intrepid9-1-1 is capable of submitting queries to a NENA i3-compliant external LIS and to the required border control function (BCF) to secure such interconnectivity and subsequent messaging. Furthermore, Intrepid9-1-1 provides location using a dereference protocol against an external third-party LIS infrastructure.

The TCS solution can exist in a number of routing states, depending upon the transitional maturity of the overall NG9-1-1 system. For example, the company's Intrepid9-1-1 IP-based selective router (SR) can deliver calls to legacy PSAPs and NG9-1-1 PSAPs. The company's IP-based call-handling solution can accept calls from legacy SRs or NG9-1-1 SRs. All that changes is the type of equipment (routers, switches, and gateways) installed at each location, and whether analog signaling is being converted to SIP, or if SIP signaling is being converted to analog.

The system currently supports the delivery of direct SIP, Signaling System 7 (SS7), analog Centralized Automatic Message Accounting (CAMA), T1 CAMA, Primary Rate Interface

(PRI)/Integrated Services Digital Network (ISDN), Plain Old Telephone Service (POTS), Private Branch Exchange (PBX), FCC Phase I and Phase II. In the event the call taker is still using a legacy system, the call is converted back into an analog format at the PSAP.

4.6 LEGACY PSAP GATEWAY (LPG)

A legacy PSAP gateway (LPG) is used to provide seamless connection to PSAP's that have not upgraded to NG9-1-1 PSAP operations.

The Legacy PSAP Gateway is a signaling and media interconnection point between an ESInet and a legacy PSAP.

It plays a role in the delivery of emergency calls that traverse an i3 ESInet to get to a legacy PSAP, as well as in the transfer and alternate routing of emergency calls between legacy PSAPs and i3 PSAPs. The LPG shall support the LoST protocol in order to provide selective transfer information (minimally police, fire and EMS) to a legacy PSAP based on the routing polygons provided by the local ECRF.

The Legacy PSAP Gateway supports an IP (i.e., SIP) interface towards the ESInet on one side, and a traditional MF or Enhanced MF interface (comparable to the interface between a traditional Selective Router and a legacy PSAP) on the other.

The Legacy PSAP Gateway also includes an ALI interface (as defined in NENA 04-001 or NENA 04-005) which can accept an ALI query from the legacy PSAP.

The LPG must then respond with location information for a call that is formatted according to the ALI interface supported by the PSAP. Respondents shall describe their solution for the LPG to support the legacy PSAP environment.

TCS Response: Comply.

If required, NENA i3-compliant LPGs can 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. 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 (urn:nena:service:sos.police) 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.

4.7 LEGACY SELECTIVE ROUTER GATEWAY (LSRG)

The primary function of an LSRG is to allow traffic from legacy Selective Router based networks to ESInets.

A Legacy Selective Router Gateway (LSRG) shall serve as the interface for legacy selective routers to terminate ISUP SS7 trunks utilizing an inter-tandem trunk group method of termination.

The LSRG shall convert the call signaling to SIP/RTP, query the existing ALI data management system to retrieve location information for the call and then route the call to the next nominal HOP based on a LoST query to an ECRF.

Additionally, the LSRG shall be able to facilitate bi-directional communications with the legacy selective routers for both voice and data (star codes) transactions.

Respondents shall include a description of the LSRG if utilized in their proposed solution to integrate the ESInet and legacy selective routing configuration. If an LSRG is not utilized, the respondent shall describe how the function of an LSRG is performed within their proposed solution.

TCS Response: Comply.

Our solution is NENA i3 compliant and, as such, is designed for legacy compatibility. Because no NG9-1-1 solution should be implemented via a "flash cut," it is imperative that both technologies operate simultaneously and seamlessly. To achieve this, we include LSRG functionally combined with the i3-compliant LNG element as part of the solution. This allows for maximum functionality between legacy PSAPs and NG9-1-1 PSAPs, and between legacy E9-1-1 systems and NG9-1-1 systems.

4.8 LOCATION VALIDATION FUNCTION (LVF)

Respondents shall propose a solution that includes an NG9-1-1 Location Validation Function (LVF) as defined in the NENA 08-003.

The LVF is generally only used for civic location validation. Geo coordinate validation has some limited use, in extreme cases, including national boundary routing scenarios, over coastal waters, etc. The primary validation is accomplished as locations are placed in a LIS.

The LVF shall be designed to respond to LVF clients within five (5) seconds. The LVF shall be capable of supporting multiple simultaneous queries of a significant amount, respondents shall describe how this is supported.

The LVF data and interfaces are similar to those used by an ECRF representing the same geographic area(s). Additionally, it must support both iterative and recursive queries to external LVF sources.

Respondents shall describe their proposed LVF implementation, with particular attention to the arrangement of the proposed components, user interface and features and the security aspects of the LVF.

TCS Response: Comply.

The TCS solution complies with Alabama's LVF requirements.

NENA Compliance

GeoLynx Spatial Router LVF is an IETF 5222 compliant LoST Server that provides the NENA i3 functional elements of ECRF/LVF as specified in NENA TSD 08-003.

Simultaneous & High Volume Requests

The GeoLynx Spatial Router LVF design is capable of handling many simultaneous and concurrent requests. It is designed to produce sub-second responses to most basic queries, and process larger requests very quickly.

The design is easily expandable and can accommodate geographic redundancy, if required. GeoComm will automatically increase capacity if response time exceeds an acceptable threshold.

Availability

To ensure the LVF proposed remains highly available, GeoLynx Spatial Router LVF will be deployed in a fully redundant single cluster manner, in a single datacenter at initial implementation. The GeoLynx Spatial Router LVF system will be provisioned using the same mechanisms and data as the 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 state requires, by implementing additional hardware to the system.

Database Synchronization with ECRF

GeoLynx Spatial Routers are LoST servers, no matter if they are being used for LVF or for ECRF. As such, they use the same GIS database, which is replicated and propagated across the system using the provisioning process.

Interfaces Supported

GeoLynx Spatial Router LVF supports the LoST interface.

Web Portals

GeoLynx Spatial Router is equipped with a dashboard for monitoring real-time statistics, load, query response behavior, and individual query contents, system wide and per server.

Documentation

The GeoLynx Spatial Router LVF can be utilized 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. GeoLynx Spatial Router supports LVF using site and/or structure layers and also address 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 Location Information Service (LIS), the address records must be validated to ensure they are adequate for routing, dispatch. This is accomplished by locating the civic address in the authoritative GIS database for the service area.

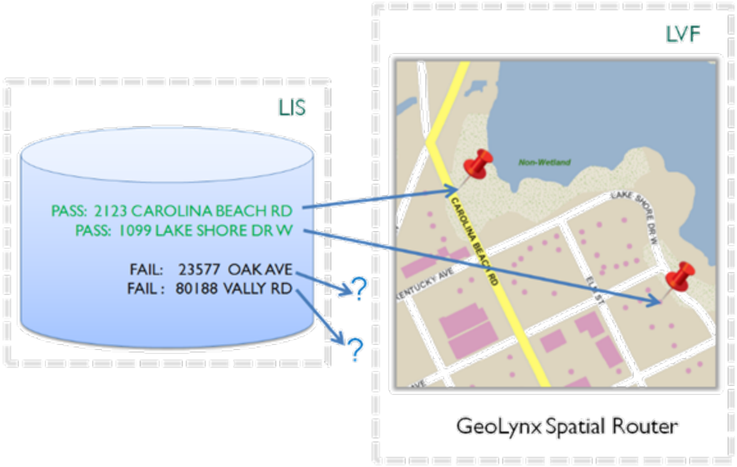


Exhibit 21. Location Validation Function

LVF queries include a validateLocation=true attribute. When this attribute is present and set true in the query, then GeoLynx Spatial Router treats the request as a location validation request, and returns a LoST <findServiceResponse> 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 GeoLynx Spatial Routers in the system whether they are being used for ECRF or LVF queries.

Features:

- IETF 5222 compliant 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

4.8.1 LOCATION SERVICES

Location is fundamental to the operation of the 9-1-1 system. Location is provided external to the ESInet, and the functional entity which provides location is a Location Information Server (LIS).

Respondents shall propose a solution that supplies a network interface to the LIS.

Respondents must include the necessary security provisions and define all communication paths between the LIS and the LVF, LSRG and LNG.

Respondents shall include a description that covers the transition from the existing routing into the LIS.

TCS Response: Comply.

TCS can interface with a LIS/CIDB functional element. We support either LbyR (Location by Reference) or LbyV (Location by Value), or both, for the processing of 9-1-1 calls originating from both legacy and IP-based networks. The LIS should support the HTTP-Enabled Location Delivery (HELD) dereference queries from i3 PSAPs. Additionally, the LIS should be extensible to support included locations from future applications such as data-only emergency call initiation generated by telematics and alarm services.

During transition to NG9-1-1, the our 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 of LbyV via SIP signaling to the i3 PSAP. The TCS solution is engineered to support a CIDB for an eventual replacement of ALI. TCS' documentation shows direct connections to the Mobile Positioning Center (MPC), Gateway Mobile Location Center (GMLC), and VoIP Positioning Center (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.

As a database function, the CIDB, with the LIS, should support NENA-referenced "Additional Call" data and the retrieval mechanism to obtain mandatory additional caller data consistent with NENA 71-001 specifications (e.g., class of service [CoS] and disability indicator). For the i3-compliant PSAP, location and additional data supplied by the LIS/CIDB will be delivered through the ESInet.

After a LIS has been implemented, GeoComm will ensure compliance with any security requirements as they are developed.

4.9 LEGACY DATABASE SERVICES

The Board recognizes that ALI database and other legacy database services (LDB) will be required for the foreseeable future.

Respondents shall include in their proposal details about their approach to ALI database connections and ALI maintenance functions as well as other any other LDB functions necessary to support the ANGEN system.

Respondents shall define how their proposed LDB service will be operated, managed and maintained for the duration of the contract.

Respondents shall also describe the PS/ALI capabilities of their solution within their proposal.

TCS Response: Comply.

TCS can supply both legacy ALI connections and an ALI replacement service, depending on the needs of the state. Legacy connections will query existing ALI databases for location information from the ESInet. If the state so elects, we can replace the legacy ALI system with our own Intrepid9-1-1 ALI database. While TCS does not offer PS/ALI services, we do support PS/ALI vendors for input of data into the ALI database using the same procedures as the originating service providers.

ALI Database Replacement Solution Summary

The legacy Automatic Location Identification (ALI) system is an integral part of the Enhanced 9-1-1 (E9-1-1) environment. Address information of an inbound call is retrieved from the ALI and displayed to the call taker. The Master Street Address Guide (MSAG) is used to format the information and as a validation source when new subscriber accounts are added. The evolution of E9-1-1 to NG9-1-1 results in the replacement of legacy ALI and MSAG databases, but the transition must be managed carefully. The TCS Intrepid9-1-1 ALI replacement solution manages current ALI/MSAG challenges while preparing for the transition from legacy ALI/MSAG to NG9-1-1 in the following ways:

- **Controlling Recurring Maintenance Costs—**TCS has engineered a solution that is both highly reliable and cost-effective to ensure a smooth and reliable transition.
- **Preparing for the Use of GIS Data—**The TCS ALI replacement solution optionally allows for the use of GIS data as the source for call routing, without affecting carrier input processes or ALI functionality. Through the careful management of GIS input data, TCS can format MSAG-like records for use in the Service Order Input (SOI) provisioning process such that Communication Service Providers (CSPs) can continue with their current Service Order Input (SOI) methods.
- **Support of Legacy E9-1-1—**The NG9-1-1 features and their benefits are superior to legacy E9-1-1 features, including in the replacement of the ALI database. However, TCS recognizes the need for replacement ALI services prior to the deployment of NG9-1-1; Intrepid9-1-1 supports a legacy ALI DBMS to address current E9-1-1 deployments while preparing for the move to NG9-1-1.

Solution Assumptions

The following assumptions provide a baseline for the ALI replacement product. Given the inherently flexible nature of the TCS solution, however, these assumptions should be taken as they are intended, as a starting point for a full solution architecture.

- TCS assumes the state desires a legacy ALI replacement product at this time, but we can also offer a solution with GIS support. If the state would rather see subscriber data reside in the NG9-1-1 database, TCS can include a LIS/CIDB in its solution that houses all the subscriber data. However, LIS/CIDB products are outside the scope of this ALI discussion.
- The TCS ALI replacement solution is configured to manage either MSAG or GIS-based data.
- For a GIS-based solution, TCS assumes the jurisdiction has a master geographic information system (GIS) database in place with the necessary layers of GIS boundaries, including PSAP boundaries, law enforcement agency boundaries, fire service area boundaries, and medical service area boundaries.
- The TCS NG9-1-1 services will be provided as a hosted model such that TCS maintains ownership of all hardware, software, and other service components.

Features of the TCS ALI Replacement Solution

TCS has structured its ALI replacement solution to utilize a percentage of NENA-defined i3 components and processes in NG9-1-1. However, as a transitory step, the state may be best served by a more traditional 9-1-1 ALI solution with processes that support NG9-1-1.

Intrepid9-1-1 delivers a combination of a traditional ALI and processes, needed today, coupled with those NENA-defined i3 components and processes that are currently applicable. The jurisdictions, local agencies, TCS, and service provider stakeholders can put the building blocks in place to add additional services as 9-1-1 stakeholders move into the NENA i3 space and/or as the State feels i3-leaning changes should be made.

TCS meets current and future ALI database challenges through its Intrepid9-1-1 ALI replacement solution, comprised of ALI DBMS and ALI Web products, as outlined in Exhibit 22.

Exhibit 22. ALI DBMS Features

Feature	Intrepid9-1-1 ALI Support
Daily Audits	X
Performs Rigorous Validation Checks on Service Orders and Manual Edits	X
NG9-1-1 Aligned	X
Enables GIS Data Source Inputs	X
Provides Access for Error Review, Statistics, and Reporting	X
Supports Service Provider Batch Edits	X
Allows Service Providers to Submit Change Requests Directly to ALI DB	X
Automated MSAG-Like Data Management Tools	X
Supports Community and Street Name Aliases	X
Provides Each Service Provider with TN Record Downloads for Data Quality Assurance	X
Provides Administrators with Full History for All TN and MSAG Records	X
Web-Based Reporting Tools	X
Built-In Data Audits	X
Service Order Fallout Reporting	X
Import/Export Standard NENA Formats	X

4.10 DISASTER RECOVERY / BUSINESS CONTINUITY

Respondents must include a disaster recovery capability within the proposed solution to offer continuity of operations in the event of a malfunction of the network, system or i3 components used to provide the primary ANGEN services.

This service must be separate and distinct in design and operation from the core ANGEN system components proposed by the Respondent.

Alternatives presented here may include the use of commercially available services and or commodity IP connections that can operate for temporary periods of time (to be determined via SLA) until normal system operations are restored to individual PSAPs or regions served by the ANGEN system.

Basic functionality must include the following at all PSAPs or locations as may be designated by the Board:

1. Receive and answer 9-1-1 voice calls via alternate hand set/desk set or other proposed device

2. Ability to Transfer via traditional landline or other means to other AL PSAPs, mirroring current PSAP transfer capabilities and practices

3. Provide for the temporary system level logging and recording of calls being processed by the disaster recovery system

TCS Response: Comply.

TCS will present a disaster recovery plan to the state of Alabama for its approval. This plan will be invoked in the event of a catastrophic failure of all, or a significant portion of, the 9-1-1 service, which will allow for the amount of time needed to repair the system or to mitigate the adverse impact of these events to public safety.

As part of TCS ISO and TL certifications, we have established an internal disaster recovery plan, fully tested the plan, update it quarterly, and practice it on a regular basis.

We will include fundamental aspects of the documentation and practice, such as:

- A discussion of possible risks to the data centers, equipment, data, and processes.
- A program to manage potential risks by eliminating them or reducing them to an acceptable level.
- A strategy to recover from threats that cannot be eliminated but can be foreseen.
- Reviews of the various risks and instructions for specific systems recovery.

Exhibit 23 depicts the table of contents from our established Disaster Recovery Plan.

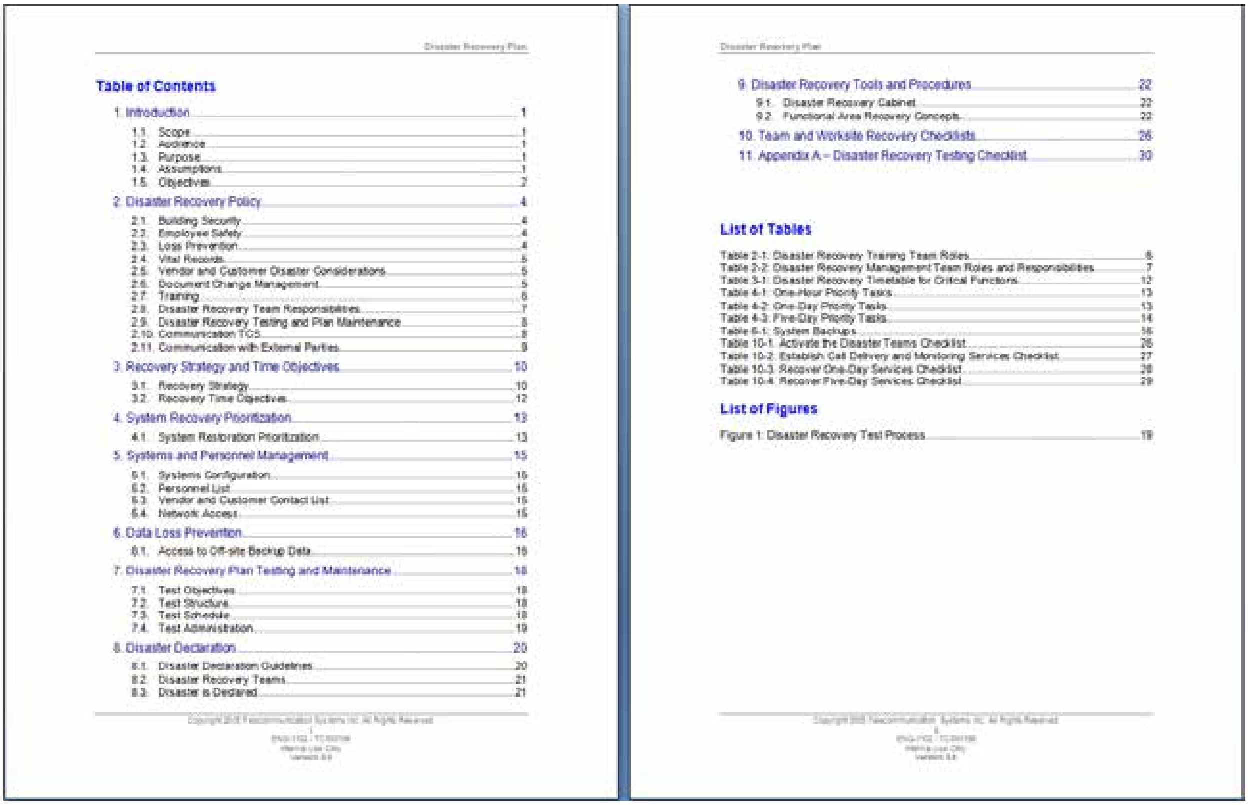


Table of Contents

1. Introduction 1
1.1. Scope 1
1.2. Audience 1
1.3. Purpose 1
1.4. Assumptions 1
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

9. Disaster Recovery Tools and Procedures 22
9.1. Disaster Recovery Cabinet 22
9.2. Functional Area Recovery Concepts 22
10. Team and Worksite Recovery Checklists 26
11. Appendix A – Disaster Recovery Testing Checklist 30

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

Exhibit 23. Table of Contents from TCS' Established Disaster Recovery Plan

Part of the disaster recovery effort involves determining if existing T1 connections to legacy selective routers are a viable, valuable addition to recovery efforts. Barring effective utilization of existing T1 circuits, we would then look to commercial carrier backup networks, wireless networks, satellite connectivity, or some other means to reestablish connectivity. The availability of any of these items is dependent upon required bandwidth, site location, and a number of other site-specific criteria that can be discussed with the state in greater detail.

SECTION 5 SYSTEM REPORTING and i3 LOGGING REQUIREMENTS

5.1 REPORTING AND DATA COLLECTION SYSTEM REQUIREMENTS

The Board requires enterprise wide reporting and data collection capabilities on all aspects of the ANGEN ecosystem.

This capability must be agnostic to provider, system or technology and must be able to collect reportable data on the operation, configuration, and maintenance of the ANGEN system regardless of function, domain, service area or provider.

Given that there may be multiple providers of components and systems that will comprise the ANGEN ecosystem, the Board will entertain stand-alone proposals from vendors who can offer an enterprise wide, multi-vendor, fully integrated solution to satisfy this requirement.

Respondents may offer enterprise wide reporting as a component of their solution as well.

The Board will not entertain proprietary, disparate or system specific reporting systems.

Respondents must be prepared to provide or support the collection and integration of an enterprise wide reporting and data collection capability.

TCS Response: Comply.

TCS is partnering with Direct Technology to provide their ECaTS reporting platform, which can provide all call handling and network reporting requirements as described by the Alabama 9-1-1 Board and contained within this RFP. The proposal assumes the following assumptions around deployment of the ECaTS reporting platform:

- An i3 based ESInet is in place, statewide, and can send logging messages to the ECaTS i3 Meta logger. ECaTS (its data collectors) will reside on the same network as the CPE and ESInet functional elements to ensure the ability to collect data from all systems.
- All call handling equipment is able to provide either an i3 based call handling log or a CDR output CDR output is assumed to contain operator/agent data in addition to all call handling fields (ex: seizure time, ring time, answer time, etc.)
- The systems on the ESInet that provide i3 logging output are conforming their log output to the Detailed Functional and Interface Specification for the NENA i3 Solution, Stage 3 Version 1.

ECaTS Solution Overview

ECaTS is an acronym for Emergency Call Tracking System. ECaTS is the first enterprise wide 911 Call Reporting and Data Collection System that leverages the ubiquitous nature of the Internet to provide secure, real-time reporting to the 911 industry. ECaTS is currently installed and in production throughout the States of California, Utah, Oregon, North Carolina, Indiana, Kansas, Delaware, parts of Texas, Florida, Kentucky, Oklahoma, Colorado, Virginia, Louisiana, Mississippi, Tennessee and Washington. Currently ECaTS provides full analysis and reporting of all 911 call/events, call taker and trunk activity throughout these States. Pending available data feeds from the CPE, the ECaTS system has the capability to support NG9-1-1 activity and statistics that can listen, record and translate NG9-1-1 events.

The Alabama 9-1-1 Board and PSAP personnel should expect to enjoy the benefits of a flexible and intuitive web based user interface, easy to use pre-configured reports, and the advanced offerings of the ad-hoc reporting tools. ECaTS provides users with the ability to report on 911 call statistics and trunk statistics across an individual PSAP, county, any given jurisdiction and/or statewide with unified reporting and managed services. ECaTS has the ability to report on all calls captured by the raw Call Detail Records (CDR) from CPE. ECaTS can be accessed by any authorized user from a web browser. Clients access their reports directly from a PC, laptop or any mobile device such as iOS, Android or Windows based systems.

ECaTS Features

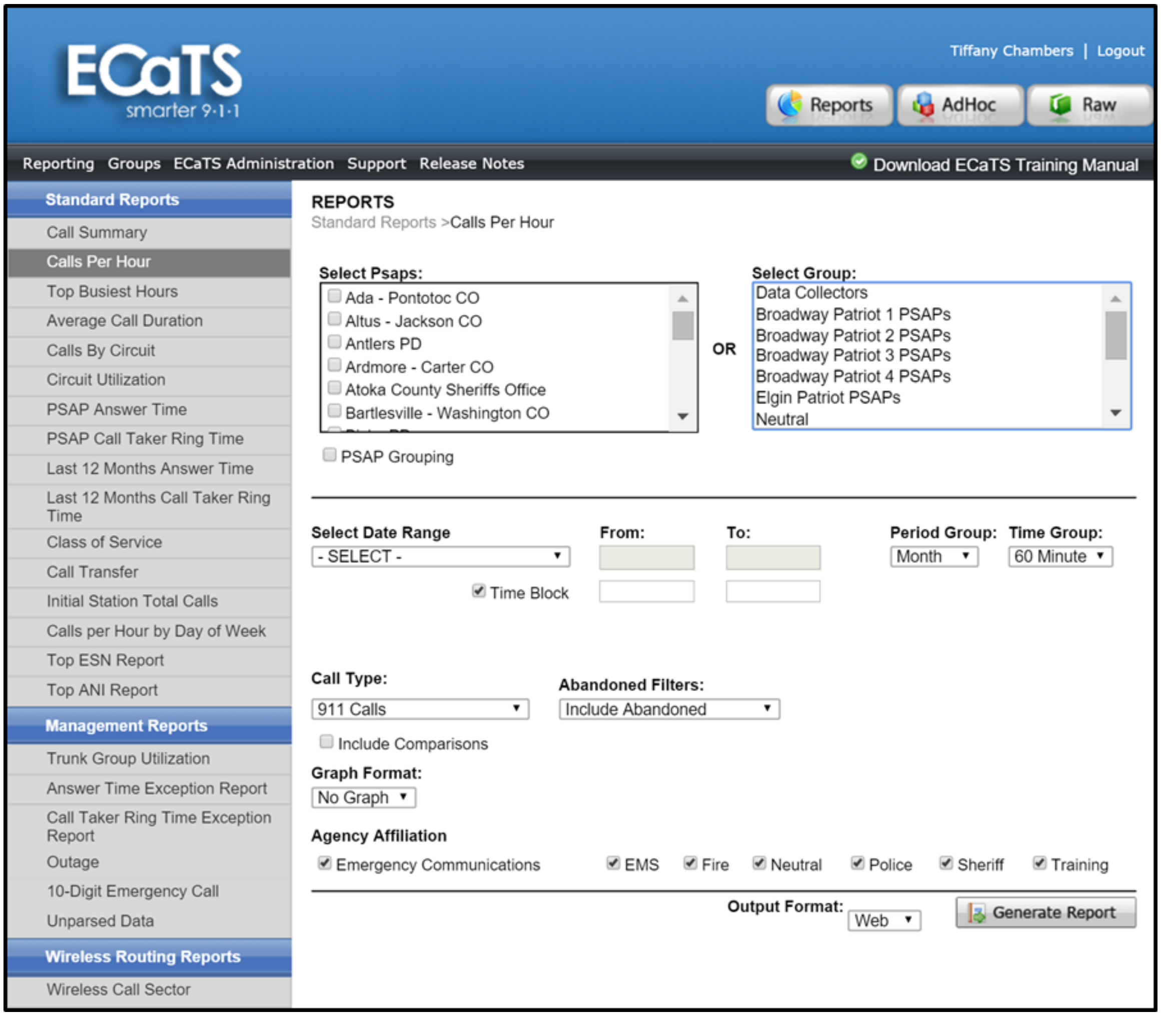
This section of the document provides the Alabama 9-1-1 Board with a high-level description of the product's key features. In essence, ECaTS provides the first universal 911 call statistics product that can transparently report all intelligence related to 911 call/event handling and volume across an individual PSAP, county, any given jurisdiction and/or statewide regardless of the Customer Premise Equipment (CPE) at the PSAP.

Intuitive Reporting Module

ECaTS was built on the concept of simplicity. Its reporting module, the heart of the application, provides the user with simple, intuitive click reporting options. Authorized users are able to generate near real-time statistics by simply selecting the report, the timeframe and a PSAP (or collection of PSAPs) to be used in the report. The system then accesses the back end servers to render the report directly to an Internet browser.

The beauty of the application is that authorized users may pull information from one PSAP, County or any given jurisdiction with the same level of simplicity. The drastic complexity of pulling information from different types of CPE manufacturers, installations or software versions located at each PSAP is completely eliminated by ECaTS.

Exhibit 24 represents the ECaTS Interface.



REPORTS
Standard Reports >Calls Per Hour

Select Psaps:
□ Ada - Pontotoc CO
□ Altus - Jackson CO
□ Antlers PD
□ Ardmore - Carter CO
□ Atoka County Sheriffs Office
□ Bartlesville - Washington CO

OR

Select Group:
Data Collectors
Broadway Patriot 1 PSAPs
Broadway Patriot 2 PSAPs
Broadway Patriot 3 PSAPs
Broadway Patriot 4 PSAPs
Elgin Patriot PSAPs
Neutral

□ PSAP Grouping

Select Date Range: - SELECT -
From:
To:
Period Group: Month
Time Group: 60 Minute
☑ Time Block

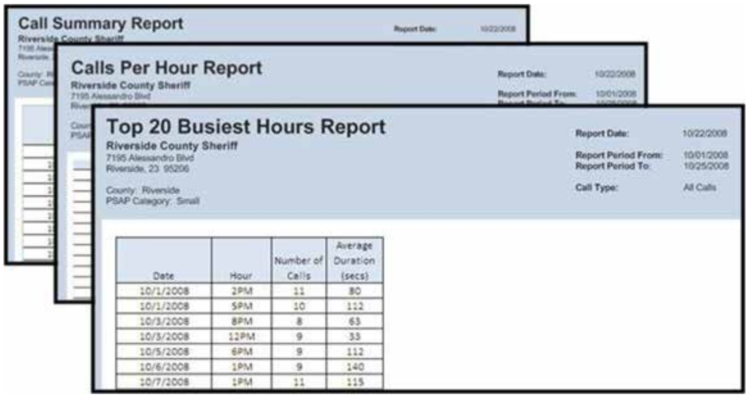
Call Type: 911 Calls
Abandoned Filters: Include Abandoned
□ Include Comparisons
Graph Format: No Graph

Agency Affiliation
☑ Emergency Communications ☑ EMS ☑ Fire ☑ Neutral ☑ Police ☑ Sheriff ☑ Training

Output Format: Web

Exhibit 24. ECaTS Interface

Generating a report is as simple as selecting the report on the left, select one, multiple or a PSAP group, selecting a date range and clicking on the Generate Report button. The Group selector is completely user created and maintain so that County Administrators may define commonly used group of PSAPs against which they normally generate reports. The user may also decide what type of graphical representation they wish to include in the report and if they want the output to be web based, PDF or directly into an Excel file for further analysis.



Call Summary Report
Riverside County Sheriff
Report Date: 10/22/2008

Calls Per Hour Report
Riverside County Sheriff
7195 Alessandro Blvd
Report Date: 10/22/2008
Report Period From: 10/01/2008

Top 20 Busiest Hours Report
Riverside County Sheriff
7195 Alessandro Blvd
Riverside, 23 95206

County: Riverside
PSAP Category: Small

Report Date: 10/22/2008

Report Period From: 10/01/2008
Report Period To: 10/25/2008

Call Type: All Calls

Date	Hour	Number of Calls	Average Duration (secs)
10/1/2008	2PM	11	80
10/1/2008	5PM	10	112
10/3/2008	8PM	8	63
10/3/2008	12PM	9	33
10/5/2008	6PM	9	112
10/6/2008	1PM	9	140
10/7/2008	1PM	11	115

Exhibit 25. Sample ECaTS Reports

Pre-Configured Reports

Many of the reports usually generated by PSAP Managers tend to seek the same level of statistical data. Information such as Call Summary Reports, Number of Calls per Hour, Top 20 Busiest Hours, Call Duration and other popular reports are easily available to the users upon logging into the system. If the report contains data for multiple PSAPs, the information can all be aggregated into one individual report. Historical trending takes a whole new meaning when a user can generate 911 Call Statistics for their jurisdiction during an entire year with just a few clicks of a mouse.

ECaTS includes the following preconfigured reports:

Standard Reports

Call Summary Report

A listing of all of the calls answered and abandoned by call type (e.g. “9-1-1” or “10 digit emergency”) for each day of the selected time frame.

Calls Per Hour Report

A listing of the number of calls delivered to the CPE controller each hour of each day for the selected time frame.

Top Busiest Hours Report

A listing of the top 20 busiest hours for any selected timeframe which includes the call count and average call duration for the selected period.

Average Call Duration Report

A listing of the number of calls each hour during the selected time frame with the queue time (average duration from trunk seizure at the PSAP to ring start, also known as Set-up Time), ring time (average duration from ring start to answer time, if equipment provides the required Ring Event), hold time (average duration calls are on hold during that hour), and talk time (average duration from answer time to disconnect time minus any hold time that occurred during the call, this is a pure talk time metric).

Calls by Circuit Report

A listing of the number of calls received on each circuit each day during the selected timeframe.

Circuit Utilization Report

A statement of the percentage of time that a given number of incoming trunks were engaged at the same time within each trunk group (trunk groups are defined by each PSAP). This report provides statistics on trunk groups allowing management to identify trunk groups that are over or under trunked.

PSAP Answer Time Report

A statement of the number of calls that were answered in 10 seconds or less, 20 seconds or less and other answer times for each hour of the selected timeframe. The summary information includes the number of calls in each answer time category and the percentage for each category. Answer time is computed between Call Seizure and call Taker Answer times.

PSAP Call Taker Ring Time Report

CPE Equipment that provides a ring time event will be able to measure call taker ring time by measuring the time between the ring event and the answer event. For the equipment that does not have this event, a false ring time factor can be introduced to simulate a single ring (usually 2 seconds) or if this is not used this report would match the PSAP answer time and measure from seizure to answer.

Last 12 Months Answer Time Report

Provides summary information for each month within a 12 month period including the number (and corresponding percentage) of calls answered in 10 seconds or less.

Last 12 Months Call Taker Ring Time Report

The Last 12 Months Call Taker Ring Time Report gives the total number of inbound, parsed calls for the last 12 full months from when the report was generated. This report, similar to the PSAP Call Taker Ring Time Report, utilizes ring times, calculated from when the call is presented to the call taker to when the call is answered (meaning that there is no set up time included in the calculations). This report provides the percentage of calls with ring seconds between 0 and 10 as well as the total number of calls answered within 10 ring seconds, per month.

Class of Service Report

A listing of the number of calls for the selected timeframe broken down by a selected subset of classes of service from the ALI data string such as business (BUSN), residential (RESD), Centrex (CNTX), PBX, pay phone, VoIP, or wireless phase 1 WPH1/W911) or phase 2 (WPH2).

Call Initial Station Total Calls Report

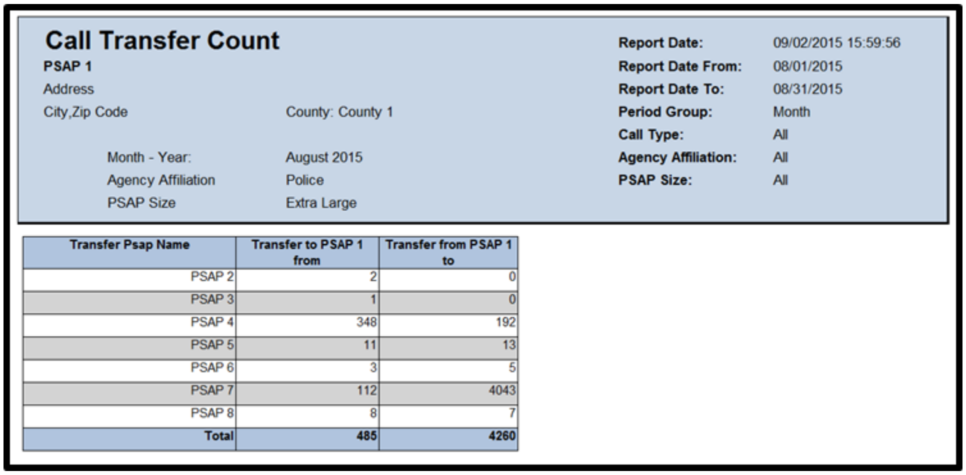
A listing of the number of calls received each hour at each answering position during the selected timeframe. Requires the source data to include the station identifier for each answered call.

Call Transfer Report

Provides details regarding every call that was transferred to or from the PSAP during the selected timeframe. Details include ANI information, trunk seizure time of call(s) at each PSAP and other relevant call information. All PSAPs must be participating in the ECaTS program to show up on the Transfer report, any secondary that is not in the ECaTS system would not appear in this report. In order to maximize call transfer report accuracy, all participating PSAPs must synchronize their system clocks with an industry standard network clock service or device. In addition, this report provides PSAP-to-PSAP transfers and does not include internal station-to-station transfers.

Call Transfer (Summary) Count Report

The Call Transfer Count report provides the user with counts for every transfer to and from the selected PSAP for the date range chosen. The report uses the same rules to determine transfers as the current transfer report.



Call Transfer Count

PSAP 1
Address
City,Zip Code   County: County 1

Month - Year: August 2015
Agency Affiliation Police
PSAP Size Extra Large

Report Date: 09/02/2015 15:59:56
Report Date From: 08/01/2015
Report Date To: 08/31/2015
Period Group: Month
Call Type: All
Agency Affiliation: All
PSAP Size: All

Transfer Psap Name	Transfer to PSAP 1 from	Transfer from PSAP 1 to
PSAP 2	2	0
PSAP 3	1	0
PSAP 4	348	192
PSAP 5	11	13
PSAP 6	3	5
PSAP 7	112	4043
PSAP 8	8	7
Total	**485**	**4260**

Exhibit 26. Call Transfer Count Report

Calls by Operator

The Calls by Operator report allows a user to identify how many calls have been answered by particular users logged into the system. This report is generated by CDR output to the RDDM. If user information is not available for a particular call, information will be directed to an "Unknown Operator" row. This category is used in any situation in which an operator name is not provided with the call, this often occurs when CDR data considers a call abandoned. This report divides the calls received in a given time frame by operator name and hour of day in military time.

Operator Speed of Answer

The Operator Speed of Answer report allows a user to identify the speed with which individual operators are answering calls. This report is generated by the CDR output. If the operator name information is not available for a particular call, calls will be directed to the "Unknown Operator" row. This report is divided into separate answer time frames. The report also will identify the total calls answered as well as the average duration of the calls in seconds.

Calls per Hour by Day of Week

The Calls per Hour by Day of Week report lists the number of calls for each hour of the day, by day of week (increments also apply). Depending on the call type selected, the Calls per Hour by Day of Week report will conform to the available data. The report also features a row with the average number of calls per day of the week.

Top ESN Report

The Top ESN report will provide frequency information on the Top ESNs for the date range selected. If multiple ESNs have the same number of calls, they will all be listed on the report. A total number of records and the average duration of those calls are also included on the report. This report will only support 911 Call Types because the ESN information will be pulled from the ALI of each call.

Top ANI Report

The Top ANIs report will provide frequency information on the Top ANIs for the date range selected. If multiple ANIs have the same number of calls, they will all be listed on the report. A total number of records included in the report, and an average duration of those calls is also included.

Graphical Capabilities

The product supports a wide range of graphical representations of the data being showcased in each report. Although the system will dynamically select the most appropriate graph type based on the data being reported, each user has the ability to change the graph type before the report is generated. Currently ECaTS supports line bars, pie charts, life graphs and stackable bars. Additional graphical support is currently being added to the application for the next version of the product.

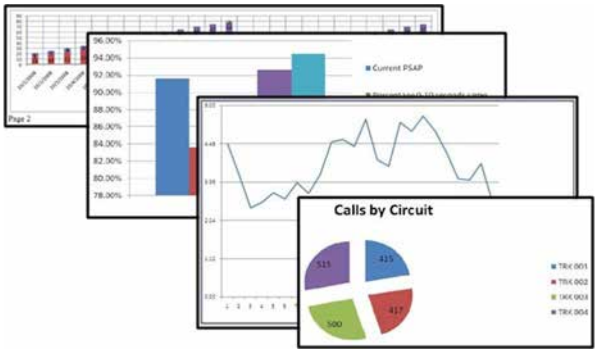


Exhibit 27. ECaTS Graphical Capabilities

Management Reports

In addition to the Call Statistics Report usually found in 911 MIS packages, ECaTS brings a wide range of Management Reports. These types of reports specifically address the analytical requirements of PSAP Managers across the industry. Management reports are available to selected authorization levels that provide tools necessary to identify areas and issues that require management attention.

ECaTS includes the following management reports:

Trunk Group Utilization Report

This report provides an in-depth analysis of call volume per trunk and trunk group. PSAP managers or coordinators can review and determine if PSAP trunks are being used at appropriate rates (e.g., are they hunting correctly, are they reaching capacity resulting in possible busy signals, etc.).

Answer time Exception Report

This report provides a clear scorecard of PSAP answering performance while clearly isolating those PSAPs that meet the National Emergency Number Association (NENA) 90/10 rule – 90 percent of the calls should be answered by each PSAP in 10 seconds or less. This report lists the PSAP(s) that answered less than 90% of calls within 10 seconds during selected time period.

Call Taker Ring Time Exception Report

This report lists the PSAPs where 90% of calls have a ring time of 10 seconds or less during selected time periods. If the selected PSAP(s) are answering 90% of calls within 10 seconds for the selected date range, the report will show ‘no data available for specified date range’.

Outage Report

This report provides the ticket number for each data monitoring alert provided by the ECaTS system. This includes call records without ALI alerts, low call volume alerts, and heartbeat alerts. A high level user will have access to the ECaTS monitoring system, allowing the user to query based on ticket number. This offers an unparalleled level of transparency into the ECaTS ticketing system, providing to the user the ability to escalate and track tickets as desired. However, it should be noted that ECaTS tracks all outages to resolution, with notification to necessary parties as determined by the customer, regardless of customer use of this report.

10-Digit Emergency Call

A listing of the 10-digit emergency circuits that exceed a predetermined level of utilization as a percentage of total 9-1-1 and 10-digit emergency calls.

Unparsed Data

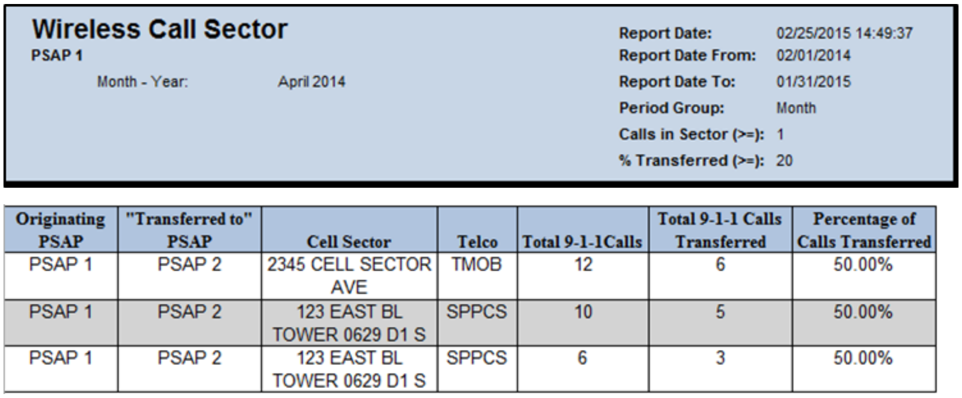
A listing of the raw data for each call that failed to meet predetermined business rules for a specific CPE manufacturer (i.e., raw data reflects disconnecting the call multiple times even though it is only answered once) or had a problem with the raw data which prevented it from being parsed (e.g., call record cut-off or interference in the data stream, causing corruption).

Wireless Routing Reports

Wireless Call Sector

The Wireless Call Sector report provides transfer information based on cell sectors for the specified date range. If a PSAP transfers 50% or more of their calls from a specific cell sector to the same destination PSAP, it will show up on this report.

Note: This report will include 9-1-1 calls, Administrative and any 10 Digit Emergency calls with ALI that meet the above requirements.



Wireless Call Sector
PSAP 1
Month - Year: April 2014

Report Date:	02/25/2015 14:49:37
Report Date From:	02/01/2014
Report Date To:	01/31/2015
Period Group:	Month
Calls in Sector (>=):	1
% Transferred (>=):	20

Originating PSAP	"Transferred to" PSAP	Cell Sector	Telco	Total 9-1-1Calls	Total 9-1-1 Calls Transferred	Percentage of Calls Transferred
PSAP 1	PSAP 2	2345 CELL SECTOR AVE	TMOB	12	6	50.00%
PSAP 1	PSAP 2	123 EAST BL TOWER 0629 D1 S	SPPCS	10	5	50.00%
PSAP 1	PSAP 2	123 EAST BL TOWER 0629 D1 S	SPPCS	6	3	50.00%

Exhibit 28. Wireless Call Sector Report

Customization

The ECaTS portal along with all pre-configured reports and functionality are fully customizable. ECaTS was built on the concept of simplicity. The ECaTS system is fully configurable to adjusting reports based on the specific standards and efficiencies required by the Alabama 9-1-1 Board. Included in the ECaTS service are five (5) pre-configured reports in addition to the standard reports or forty (40) hours of development work, which ever come first. This provides our customers with initial customization at no additional cost. Please reference the Cost Proposal for the development cost outside of the forty free hours of customization. As an option to the RFP, bundles of customization hours are provided to the Alabama 9-1-1 Board to give the ability to procure customization hours at close to wholesale costs as described in Attachment C, Cost Proposal.

Open Architecture

It should be noted that ECaTS is built using industry standard open architecture which ensures its ability to interoperate with other technologies including CPE vendors, Network Providers, Telecommunication Providers, Data and Voice recorders and others. Currently ECaTS provides multiple methodologies for interoperability from direct physical interfaces to more complex logical interfaces that leverage the i3 standards for collection, recording and storage of i3 events.

5.2 STATEWIDE STATISTICAL MONITORING

5.2.1 SYSTEM SPECIFIC REQUIREMENTS:

The proposed reporting and data collection system must provide for secure user ID login and password with the ability to enforce minimal password requirements and require password changes on a predetermined interval.

The proposed reporting and data collection system must support role based access:

- Allowing statewide users to have access to reports for the entire State.
- Allowing some users to have access to PSAP(s) report information only.
- Allowing other users to have both PSAP and ECD Manager level access to report information.

- Allowing functionality/data to show only to certain users and not to everyone.

The proposed reporting and data collection system must allow for the scheduling of automatic report generation and delivery by email as attachments to one or more recipients in a format selected by the recipient.

TCS Response: Comply.

Role Based Accessibility

ECaTS provides a secure user ID login and password based on each user's specific role. The system has the ability to enforce minimal password length and complexity as well as password changes.

The Alabama 9-11 Board will be requested to provide the assigned roles and responsibility per user in the ECaTS portal. ECaTS has the ability to add functionality and take functionality away based on a specific role. For example, a County Director's login will have access to all PSAPs within their county while a PSAP Manager's login will only have access to their specific PSAP within the County. ECaTS is only accessible via assigned usernames and passwords. Exhibit 29 is a picture of the ECaTS login screen:

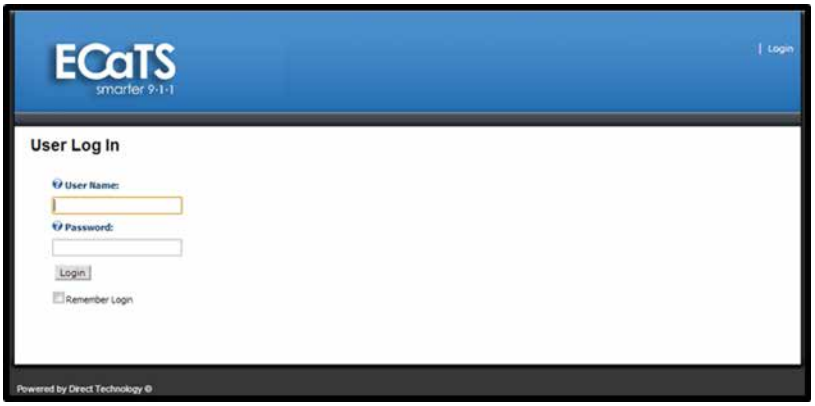


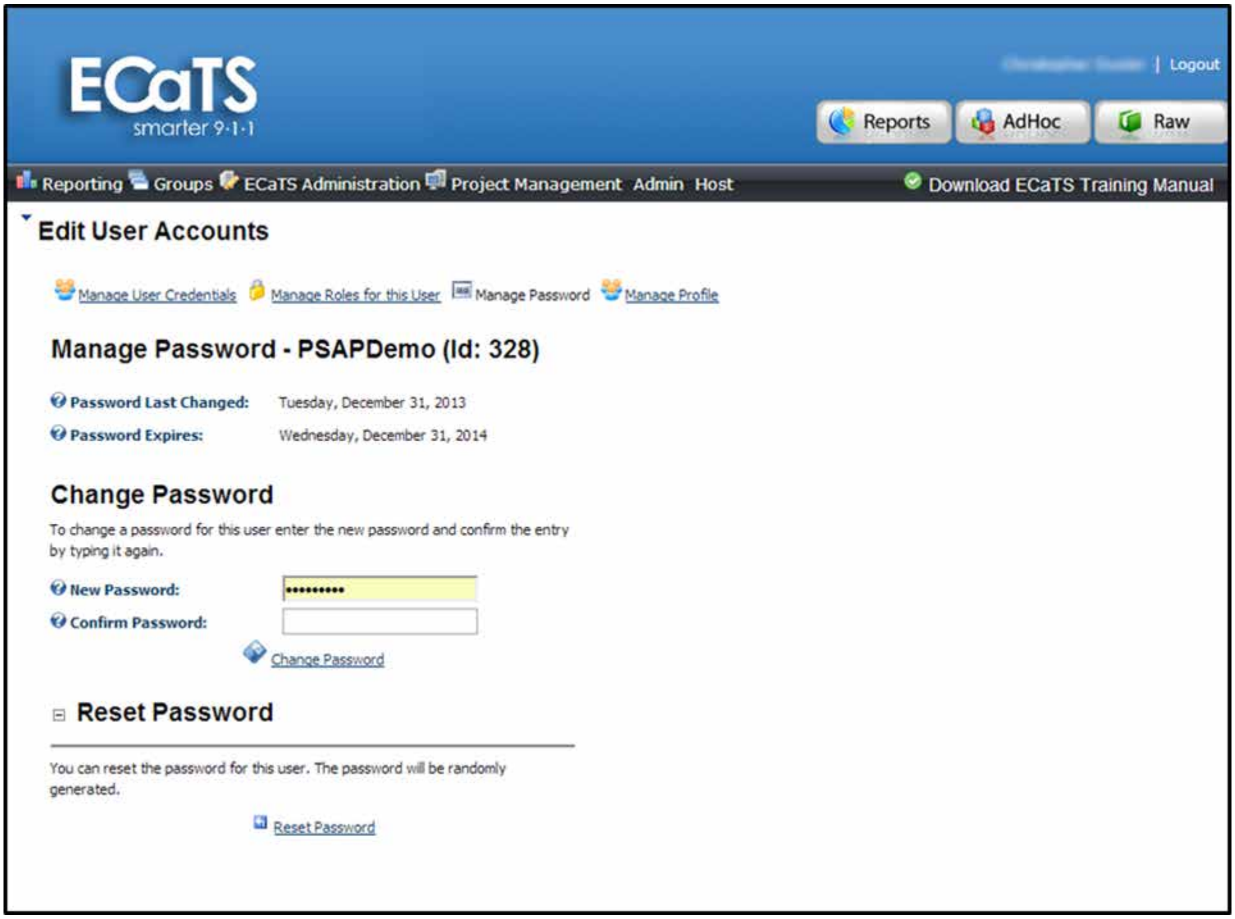
Exhibit 29. ECaTS User Login Screen

ECaTS reporting functionality is governed by 'roles' and 'PSAP groups' that determine which section(s), subsection, data and PSAPs each user may view/report on. The ECaTS system uses a custom Access Control List (ACL) used to associate individual users with particular functions and PSAP(s) that they can report against. Authentication is provided through a username/password combination required at the web site. Users have the ability to update their passwords and changes are required on a configurable rotation setting. Once authenticated, the user authorization occurs through a use of roles and user groups to assign the user to a particular reporting group and control what types of reporting the user is able to access (for example hiding management reports from a non-management users). Each action done in ECaTS can be logged by the platforms optional Audit Module (available for an additional license cost) which records all standard, ad-hoc and raw data views done by a user.

Password Management

ECaTS provides secure user ID logins and passwords with the ability to enforce minimal password requirements. ECaTS can be configured to require password expiration at any interval.

Exhibit 30 shows the password management system and a note that the password is set to expire after 12 months. The Alabama 9-1-1 Board can choose any interval required of their security doctrines.



Edit User Accounts

Manage Password - PSAPDemo (Id: 328)

Password Last Changed: Tuesday, December 31, 2013

Password Expires: Wednesday, December 31, 2014

Change Password

To change a password for this user enter the new password and confirm the entry by typing it again.

New Password: ••••••••••

Confirm Password:

Change Password

⊟ Reset Password

You can reset the password for this user. The password will be randomly generated.

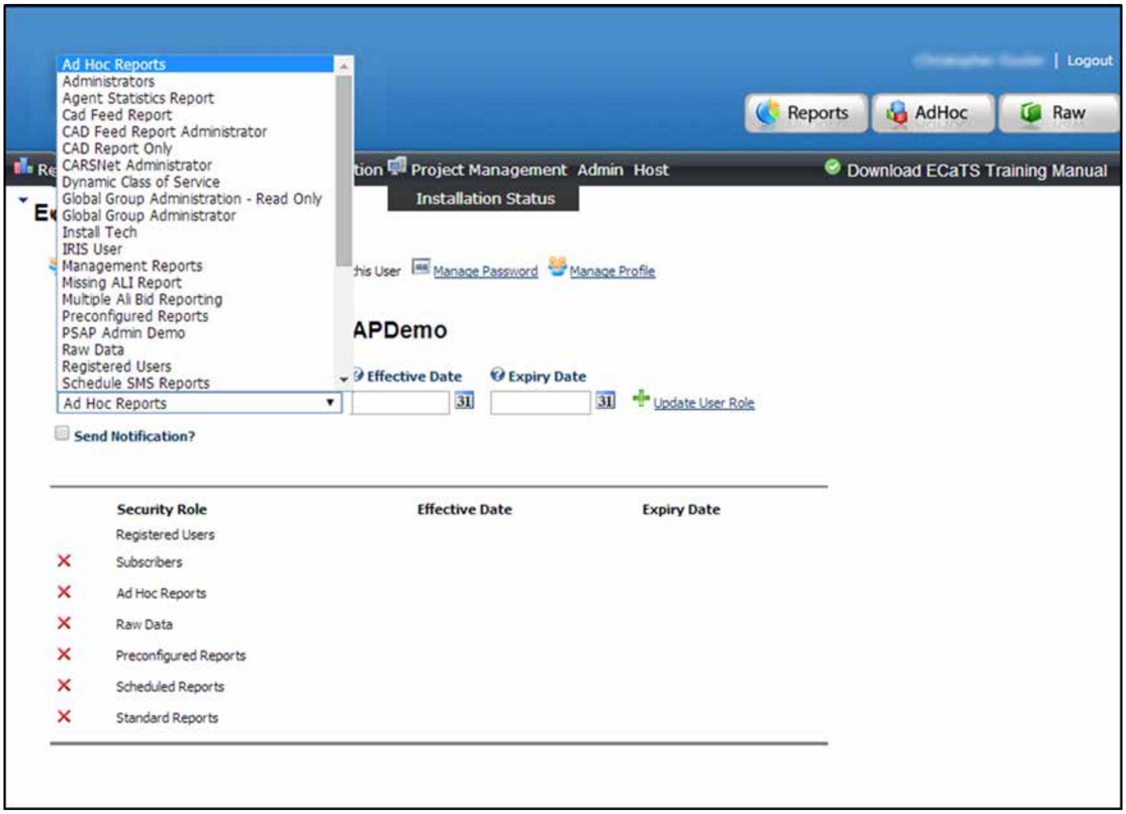
Reset Password

Exhibit 30. Password Management System

Requirements

- Allowing functionality to show only to certain users and not to everyone.
- Allowing some users to have access to PSAP report information only.

ECaTS has the ability to show specific functionality to certain users and not to everyone based on their role. The ECaTS solution has a comprehensive role system that controls individual user access to various sections of the system. By adding/removing roles from users access to various parts of the system can be controlled. Exhibit 31 below shows the role system and a sample user with six reporting roles and a displayed drop down menu with more roles that provide additional system access and functionality.



APDemo

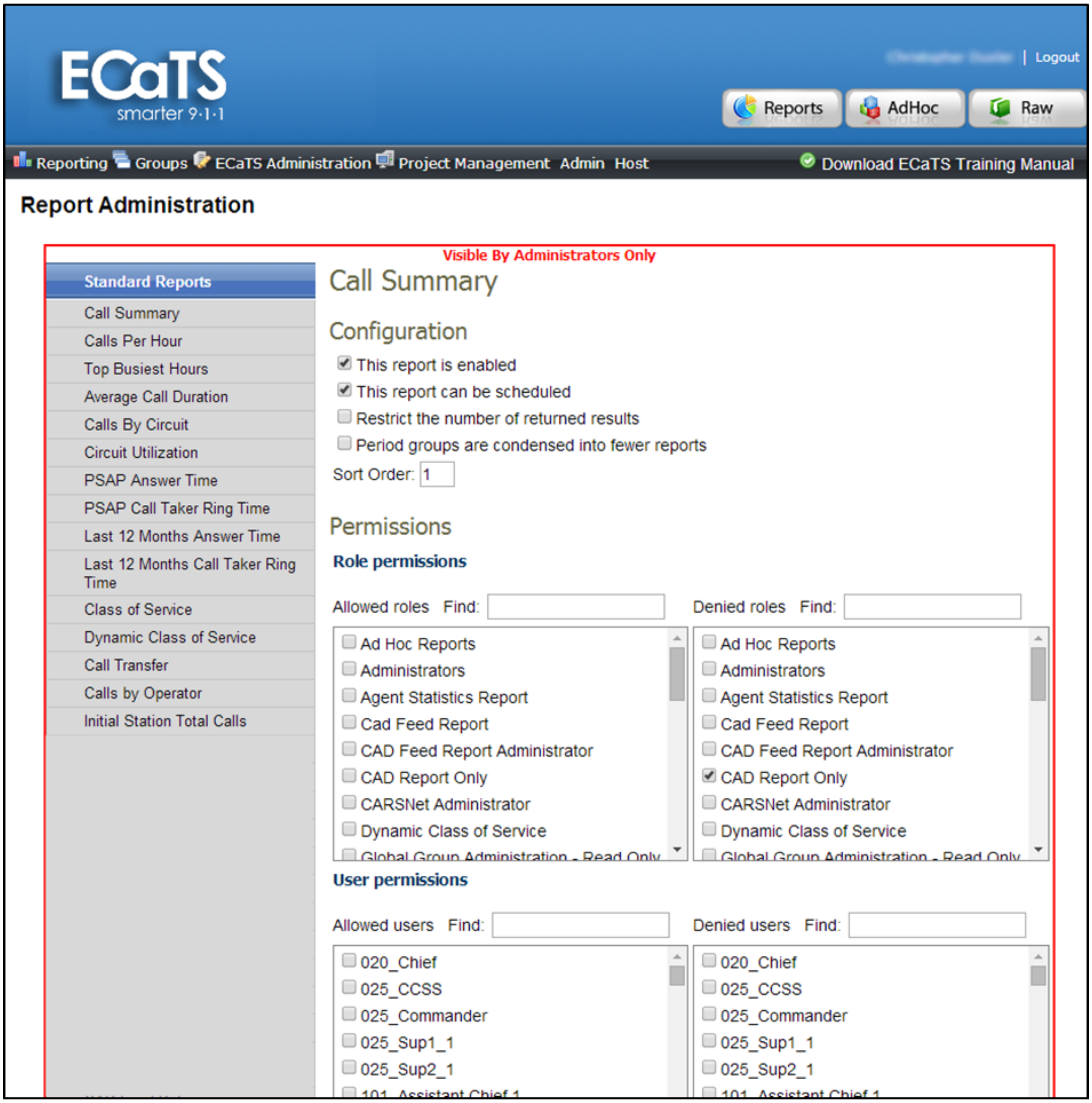
Ad Hoc Reports	Effective Date	Expiry Date
Ad Hoc Reports ▾	31	31

□ Send Notification?

	Security Role	Effective Date	Expiry Date
	Registered Users		
✕	Subscribers		
✕	Ad Hoc Reports		
✕	Raw Data		
✕	Preconfigured Reports		
✕	Scheduled Reports		
✕	Standard Reports		

Exhibit 31. User Role Management Administration

Finally, Exhibit 32 shows the interface of the Report Access Control System which provides additional control over individual reports and the users/roles that can access the reports. Combined; the role system and report management system provides administrative control to the report and function level as required by the State of Alabama.



Report Administration

Visible By Administrators Only

Standard Reports

- Call Summary
- Calls Per Hour
- Top Busiest Hours
- Average Call Duration
- Calls By Circuit
- Circuit Utilization
- PSAP Answer Time
- PSAP Call Taker Ring Time
- Last 12 Months Answer Time
- Last 12 Months Call Taker Ring Time
- Class of Service
- Dynamic Class of Service
- Call Transfer
- Calls by Operator
- Initial Station Total Calls

Call Summary

Configuration

☑ This report is enabled
☑ This report can be scheduled
☐ Restrict the number of returned results
☐ Period groups are condensed into fewer reports
Sort Order: 1

Permissions

Role permissions

Allowed roles Find:	Denied roles Find:
☐ Ad Hoc Reports	☐ Ad Hoc Reports
☐ Administrators	☐ Administrators
☐ Agent Statistics Report	☐ Agent Statistics Report
☐ Cad Feed Report	☐ Cad Feed Report
☐ CAD Feed Report Administrator	☐ CAD Feed Report Administrator
☐ CAD Report Only	☑ CAD Report Only
☐ CARSNet Administrator	☐ CARSNet Administrator
☐ Dynamic Class of Service	☐ Dynamic Class of Service
☐ Global Group Administration - Read Only	☐ Global Group Administration - Read Only

User permissions

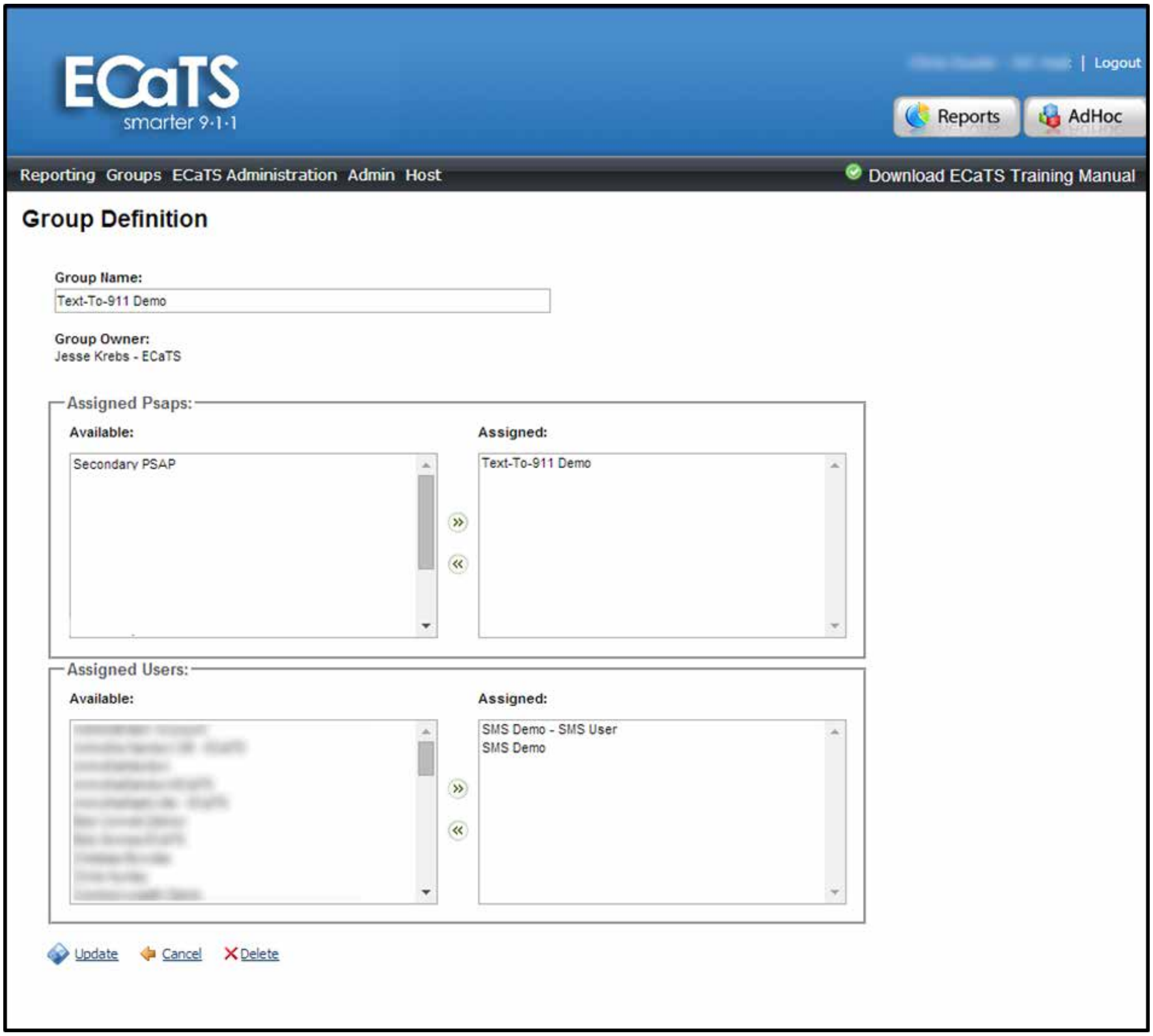
Allowed users Find:	Denied users Find:
☐ 020_Chief	☐ 020_Chief
☐ 025_CCSS	☐ 025_CCSS
☐ 025_Commander	☐ 025_Commander
☐ 025_Sup1_1	☐ 025_Sup1_1
☐ 025_Sup2_1	☐ 025_Sup2_1
☐ 101_Assistant Chief 1	☐ 101_Assistant Chief 1

Exhibit 32. Report Access Control System

Requirements

- Allowing statewide users to have access to reports for the entire State.
- Allowing other users to have both PSAP and ECD Manager level access to report information.

ECaTS provides the ability for statewide users to have access to reports for the entire State while other users have both PSAP and County level access to report information. Exhibit 33 on the following page shows the ECaTS PSAP Access Group Management System. This administrative interface associates individual users with single or groups of PSAPs to generate reports on. Users can be assigned to either individual PSAPs or in a PSAP group that has more than one PSAP. Control of which PSAPs the user can access are defined by the Alabama 9-1-1 Board and only those PSAPs the user has been approved for access will be available for reporting.


ECaTS
smarter 9-1-1
[redacted] | Logout
Reports
AdHoc
Reporting Groups ECaTS Administration Admin Host
Download ECaTS Training Manual
»
«
»
«
Update
Cancel
Delete

Group Definition

Group Name:
Text-To-911 Demo

Group Owner:
Jesse Krebs - ECaTS

Assigned Psaps:

Available:	Assigned:
Secondary PSAP	Text-To-911 Demo

Assigned Users:

Available:	Assigned:
[redacted]	SMS Demo - SMS User SMS Demo

Exhibit 33. PSAP Group Access Management

Requirement: The proposed reporting and data collection system must allow scheduling of automatic report generation and delivery by email as attachments to one or more recipients in a format selected by the recipient.

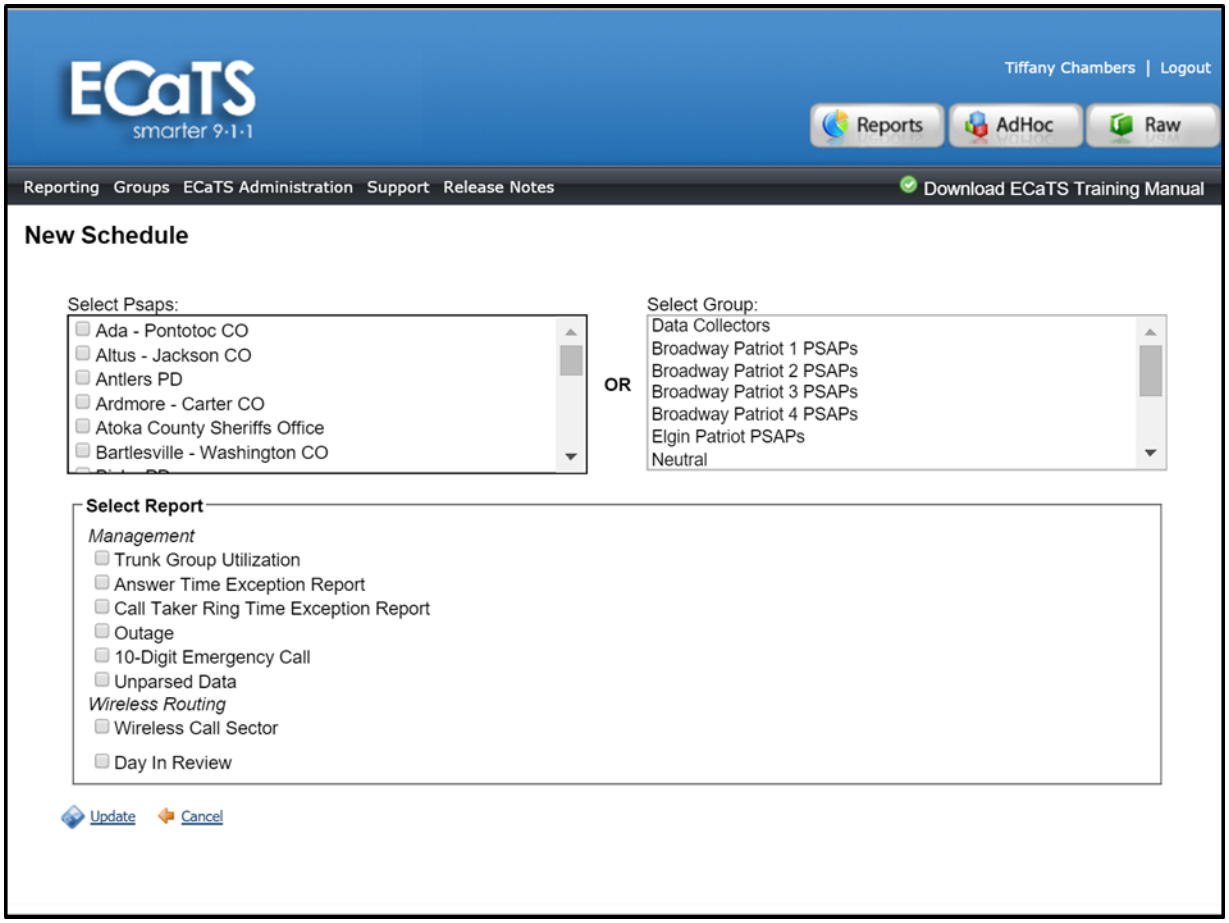
Scheduled Reports

ECaTS users have the ability to schedule reports to be automatically rendered and sent directly to their email. Management level reports are available to specific authorization levels on a regular or scheduled basis. Authorized users are advised via e-mail notification that monthly reports are available one or two days following the end of each month.

One scheduled report that has become quite popular with PSAP managers (and can be made available to standard users) is the “Day in Review” report. This report provides a snapshot of PSAP activity and is delivered to users via e-mail at the end of each day. The Day in Review report includes the following information for the day:

- Total Number of 911 Calls Received
- Total Number of 911 Calls Answered
- Total Number of 911 Abandoned Calls
- Total Abandoned 911 Call %
- Total Abandoned 911 Call % at Workstation
- Average Call Duration of the 911 Calls
- Statistics on PSAP Answer Time Performance
- Listing of the five busiest hours of the day and the number of calls each of those hours (911 Call Only)
- Listing of the five busiest hours of the day and the number of calls each of those hours (All Call Types)

Along with the Day-In-Review email, users can sign up through the ECaTS portal to have all or selected Management Reports scheduled to email as well. ECaTS has the capability to have both pre-configured and management reports scheduled and sent to the user, therefore eliminating the need to render reports daily unless needed.



New Schedule

Select Psaps:

- □ Ada - Pontotoc CO
- □ Altus - Jackson CO
- □ Antlers PD
- □ Ardmore - Carter CO
- □ Atoka County Sheriffs Office
- □ Bartlesville - Washington CO

OR

Select Group:

Data Collectors
Broadway Patriot 1 PSAPs
Broadway Patriot 2 PSAPs
Broadway Patriot 3 PSAPs
Broadway Patriot 4 PSAPs
Elgin Patriot PSAPs
Neutral

Select Report

Management

- □ Trunk Group Utilization
- □ Answer Time Exception Report
- □ Call Taker Ring Time Exception Report
- □ Outage
- □ 10-Digit Emergency Call
- □ Unparsed Data

Wireless Routing

- □ Wireless Call Sector

- □ Day In Review

Update Cancel

Exhibit 34. Schedule Report Interface

Reports can be generated in the web-browser, in a PDF format, or Excel format. These reports can be saved, emailed, and printed in the user's format of choice and accessible by any ECaTS user based on their role anytime anywhere.

5.2.2 DATA CAPTURING REQUIREMENTS:

The proposed reporting and data collection system must provide the following:

- Ability to electronically capture and buffer Call Detail Records (CDR) for each individual PSAP.
- Ability to securely capture call, text and operational data using a reliable capture method
- Ability of a buffering device to batch CDR payload, time stamp it, encrypt it and deliver the CDR data using a secure and encrypted methodology.
- Ability to provide multi-level reporting including: PSAP, ECD/County or Statewide level.
- Ability to seamlessly report PSAP, ECD/County and State's 9-1-1 call statistics from one web-based location regardless of the CPE installed at PSAPs or other hosted locations.
- Ability to export reports in PDF, HTML, CVS and Excel formats
- Ability to generate universal reports from anywhere with an Internet connection and accessible on any devices with an internet browser, i.e. iPad, iPhones, iOS, Android or Windows based systems, laptops and desktops.

- Ability to analyze ANGEN's overall 9-1-1 system performance
- Ability to provide a color coded map view of the State's System Health for all PSAPs in the State.

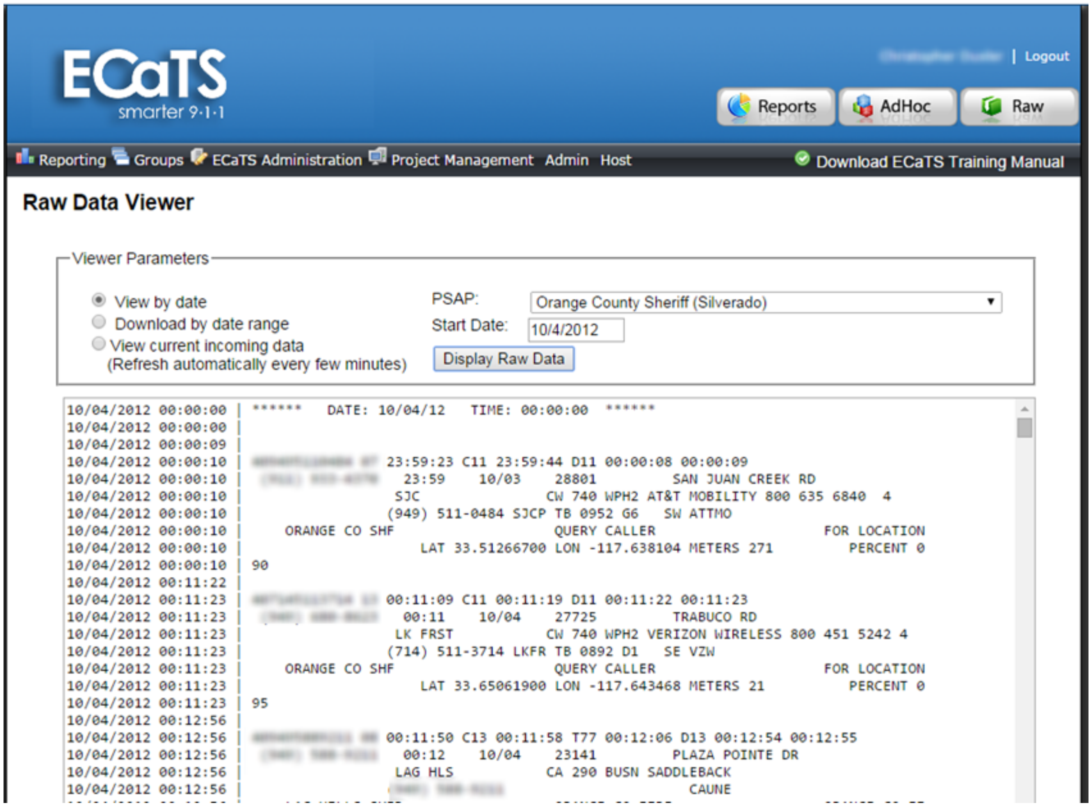
TCS Response: Comply.

Requirement: Ability to electronically capture and buffer Call Detail Records (CDR) for each individual PSAP.

Raw Data Collection and Access

Through the ECaTS Raw Data Viewer the user has access to all raw CDR records at their PSAP/PSAPs from the time of inception in electronic format. The CDR and ALI data is archived and stored at our datacenter for storing and reporting purposes, providing PSAP Managers with access to all archived data remotely online using the ECaTS web portal. By using the Raw Data Viewer portion of the interface, ECaTS allows the users to pull Raw Data from any day and from any PSAP that the user has access into.

Exhibit 35 provides an example of the Raw Data Viewer interface:



Raw Data Viewer

Viewer Parameters

● View by date
○ Download by date range
○ View current incoming data
(Refresh automatically every few minutes)

PSAP: Orange County Sheriff (Silverado)
Start Date: 10/4/2012
Display Raw Data

```
10/04/2012 00:00:00 | ******   DATE: 10/04/12   TIME: 00:00:00  ******
10/04/2012 00:00:00 |
10/04/2012 00:00:09 |
10/04/2012 00:00:10 | [redacted] 23:59:23 C11 23:59:44 D11 00:00:08 00:00:09
10/04/2012 00:00:10 |  [redacted]   23:59    10/03    28801         SAN JUAN CREEK RD
10/04/2012 00:00:10 |                 SJC              CW 740 WPH2 AT&T MOBILITY 800 635 6840  4
10/04/2012 00:00:10 |                (949) 511-0484 SJCP TB 0952 G6   SW ATTMO
10/04/2012 00:00:10 |    ORANGE CO SHF                 QUERY CALLER                     FOR LOCATION
10/04/2012 00:00:10 |                    LAT 33.51266700 LON -117.638104 METERS 271         PERCENT 0
10/04/2012 00:00:10 | 90
10/04/2012 00:11:22 |
10/04/2012 00:11:23 | [redacted] 00:11:09 C11 00:11:19 D11 00:11:22 00:11:23
10/04/2012 00:11:23 |  [redacted]   00:11    10/04    27725         TRABUCO RD
10/04/2012 00:11:23 |                 LK FRST          CW 740 WPH2 VERIZON WIRELESS 800 451 5242 4
10/04/2012 00:11:23 |                (714) 511-3714 LKFR TB 0892 D1   SE VZW
10/04/2012 00:11:23 |    ORANGE CO SHF                 QUERY CALLER                     FOR LOCATION
10/04/2012 00:11:23 |                    LAT 33.65061900 LON -117.643468 METERS 21          PERCENT 0
10/04/2012 00:11:23 | 95
10/04/2012 00:12:56 |
10/04/2012 00:12:56 | [redacted] 00:11:50 C13 00:11:58 T77 00:12:06 D13 00:12:54 00:12:55
10/04/2012 00:12:56 |  [redacted]   00:12    10/04    23141         PLAZA POINTE DR
10/04/2012 00:12:56 |                 LAG HLS          CA 290 BUSN SADDLEBACK
10/04/2012 00:12:56 |                [redacted]                 CAUNE
```

Exhibit 35. Raw CDR Viewer Interface

The reader should note, that all the CDR output is stored in its original format for auditing purposes. All the information, cradle to grave regarding calls, ALI and ANI results, etc. is stored as is and provided back to the user in the same chronological order as received by the buffering equipment.

Additionally, ECaTS allows the user to preview all generated reports on-screen before saving, printing or emailing. Once report parameters have been identified the user can select web, excel or PDF output types.

Requirement: Ability to securely capture call, text and operational data using a reliable capture method

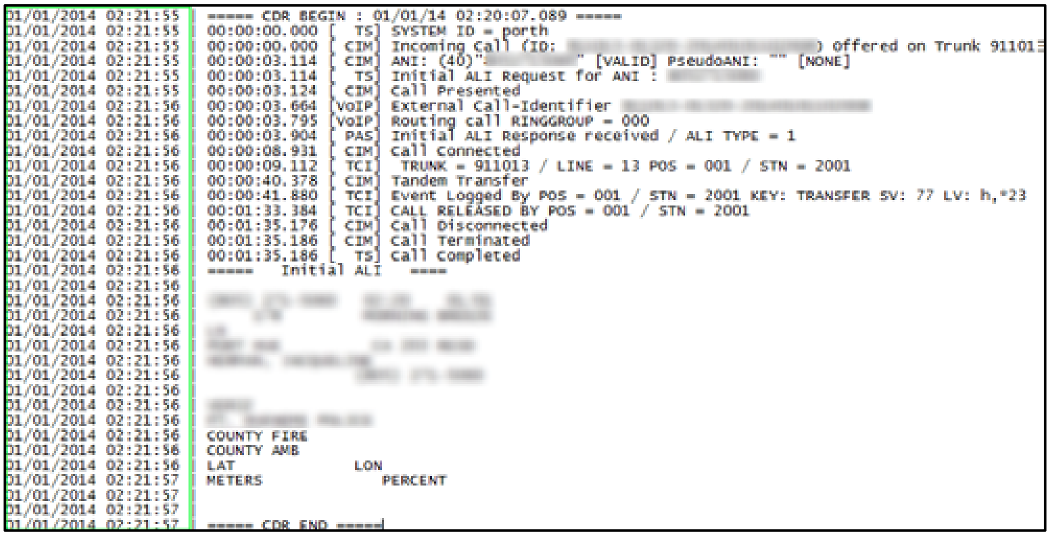
Data Collection

The RDDM has been custom built by ECaTS to satisfy the rigorous data collection needs of the 911 call center. Each device is running a special custom software stack created by ECaTS which can run either on Linux or Windows based RDDM's. The software provides the capture, compression and storage of all the data and also transmits the data over a secure SFTP connection to the ECaTS cloud. Finally, the RDDM software has been specifically designed to maintain the captured data in its raw form and to only "store and forward" the data, not do any analysis or manipulation. In addition to capturing CDR, the RDDMs have the ability to connect to other devices such as ALI controllers, CAD systems, Network Devices, PBXs, etc. This flexibility allows ECaTS to collect and report on other data points should the State of Alabama require this at a later date.

Requirement: Ability of the buffering device to batch CDR payload, stamp it with capture time, encrypt it and deliver the CDR data using a secure and encrypted methodology.

The RDDM automatically places a time stamp on any collected CDR record, regardless as to the method of collection (RS-232 or IP). The data itself is compressed and stored in a zip file and when transmitted is done over a secure SFTP connection via an SSH tunnel using strong encryption. This can be further encrypted by utilizing an encrypted point-to-point VPN tunnel between the RDDM location and the ECaTS cloud. Exhibit 36 and Exhibit 37 are samples of CDR data collected by an ECaTS RDDM which also illustrates the time stamp that is provided on each collected record. If you examine the samples below closely (Viper and Vesta 4.x presented – personal information has been blurred) you will notice there is a time stamp followed by the "|" (pipe) character. The timestamp to the left of the "|" (pipe, outlined in green) represents collection time and is provided by the RDDM, while the data to the right of the "|" (pipe) is the RAW CDR as collected and unchanged.

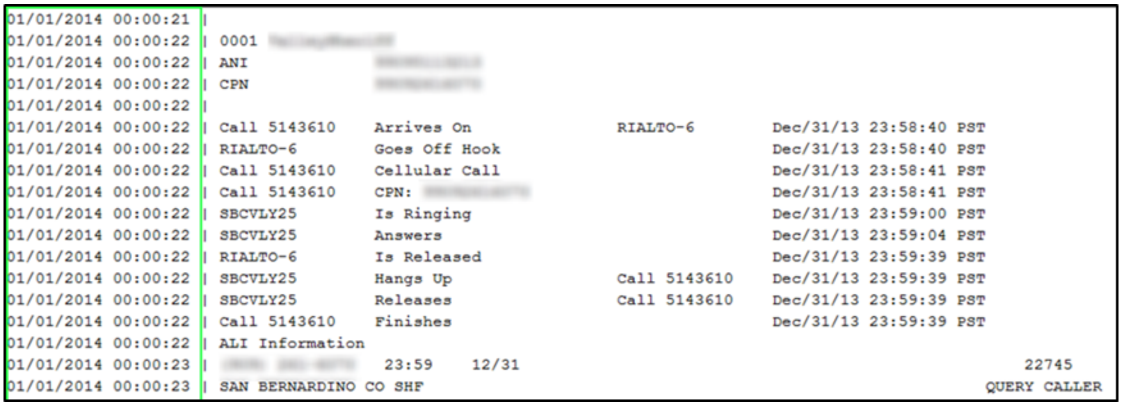
Viper



```
01/01/2014 02:21:55 | ===== CDR BEGIN : 01/01/14 02:20:07.089 =====
01/01/2014 02:21:55 | 00:00:00.000 [   TS] SYSTEM ID = porth
01/01/2014 02:21:55 | 00:00:00.000 [  CIM] Incoming Call (ID: [redacted]) Offered on Trunk 91101
01/01/2014 02:21:55 | 00:00:03.114 [  CIM] ANI: (40)"[redacted]" [VALID] PseudoANI: "" [NONE]
01/01/2014 02:21:55 | 00:00:03.114 [   TS] Initial ALI Request for ANI : [redacted]
01/01/2014 02:21:55 | 00:00:03.124 [  CIM] Call Presented
01/01/2014 02:21:56 | 00:00:03.664 [VoIP] External Call-Identifier [redacted]
01/01/2014 02:21:56 | 00:00:03.795 [VoIP] Routing call RINGGROUP = 000
01/01/2014 02:21:56 | 00:00:03.904 [  PAS] Initial ALI Response received / ALI TYPE = 1
01/01/2014 02:21:56 | 00:00:08.931 [  CIM] Call Connected
01/01/2014 02:21:56 | 00:00:09.112 [  TCI]  TRUNK = 911013 / LINE = 13 POS = 001 / STN = 2001
01/01/2014 02:21:56 | 00:00:40.378 [  CIM] Tandem Transfer
01/01/2014 02:21:56 | 00:00:41.880 [  TCI] Event Logged By POS = 001 / STN = 2001 KEY: TRANSFER SV: 77 LV: h,*23
01/01/2014 02:21:56 | 00:01:33.384 [  TCI] CALL RELEASED BY POS = 001 / STN = 2001
01/01/2014 02:21:56 | 00:01:35.176 [  CIM] Call Disconnected
01/01/2014 02:21:56 | 00:01:35.186 [  CIM] Call Terminated
01/01/2014 02:21:56 | 00:01:35.186 [   TS] Call Completed
01/01/2014 02:21:56 | =====   Initial ALI   ====
01/01/2014 02:21:56 |
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 |
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | [redacted]
01/01/2014 02:21:56 | COUNTY FIRE
01/01/2014 02:21:56 | COUNTY AMB
01/01/2014 02:21:56 | LAT            LON
01/01/2014 02:21:57 | METERS            PERCENT
01/01/2014 02:21:57 |
01/01/2014 02:21:57 |
01/01/2014 02:21:57 | ===== CDR END =====
```

Exhibit 36. Raw CDR Collected from Viper

Sentinel/Vesta 4.x



```
01/01/2014 00:00:21 |
01/01/2014 00:00:22 | 0001 [redacted]
01/01/2014 00:00:22 | ANI              [redacted]
01/01/2014 00:00:22 | CPN              [redacted]
01/01/2014 00:00:22 |
01/01/2014 00:00:22 | Call 5143610    Arrives On            RIALTO-6        Dec/31/13 23:58:40 PST
01/01/2014 00:00:22 | RIALTO-6        Goes Off Hook                         Dec/31/13 23:58:40 PST
01/01/2014 00:00:22 | Call 5143610    Cellular Call                         Dec/31/13 23:58:41 PST
01/01/2014 00:00:22 | Call 5143610    CPN: [redacted]                       Dec/31/13 23:58:41 PST
01/01/2014 00:00:22 | SBCVLY25        Is Ringing                            Dec/31/13 23:59:00 PST
01/01/2014 00:00:22 | SBCVLY25        Answers                               Dec/31/13 23:59:04 PST
01/01/2014 00:00:22 | RIALTO-6        Is Released                           Dec/31/13 23:59:39 PST
01/01/2014 00:00:22 | SBCVLY25        Hangs Up              Call 5143610    Dec/31/13 23:59:39 PST
01/01/2014 00:00:22 | SBCVLY25        Releases              Call 5143610    Dec/31/13 23:59:39 PST
01/01/2014 00:00:22 | Call 5143610    Finishes                              Dec/31/13 23:59:39 PST
01/01/2014 00:00:22 | ALI Information
01/01/2014 00:00:23 | [redacted]    23:59    12/31                                          22745
01/01/2014 00:00:23 | SAN BERNARDINO CO SHF                                              QUERY CALLER
```

Exhibit 37. Raw CDR Collected from Sentinel/Vesta

Requirement: Ability to provide multi-level reporting including: PSAP, ECD/County or Statewide level.

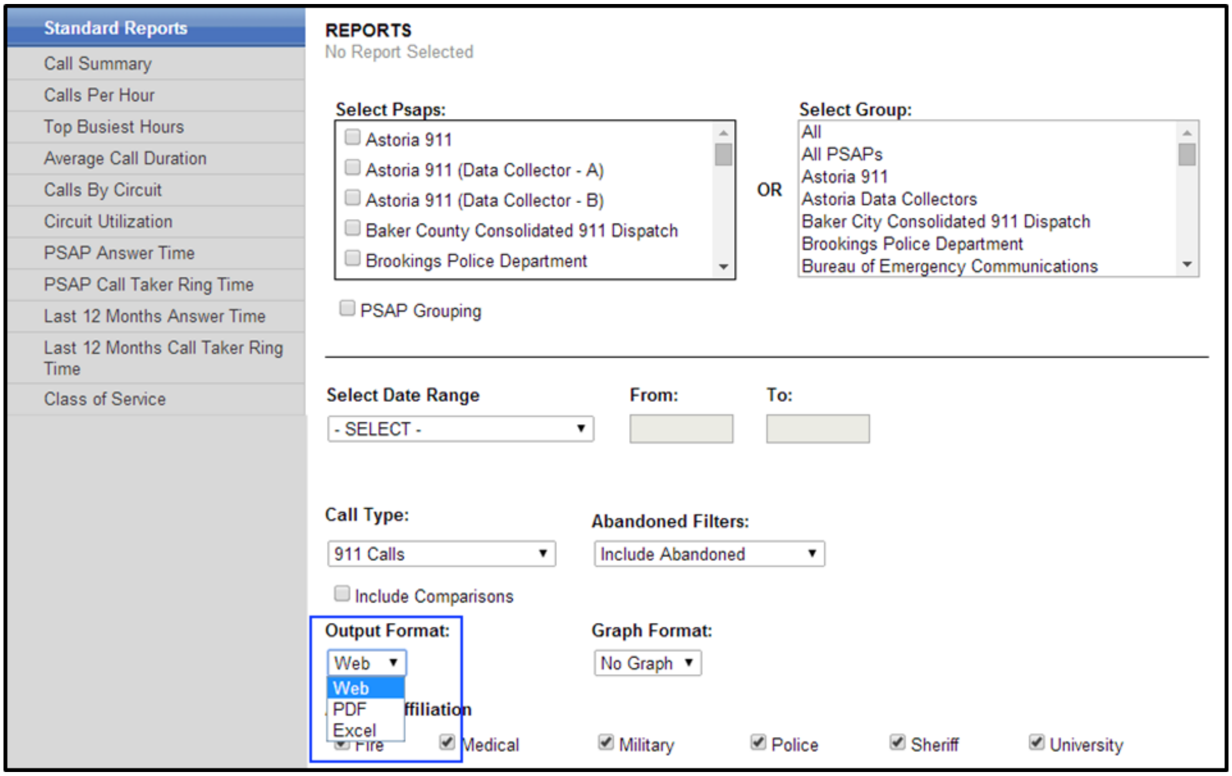
The ECaTS platform was designed for multi-level reporting across multiple different CPE platforms. The ability to render reports across PSAPs, counties, or statewide is a fundamental feature of the product. In addition, comparative reporting at multiple levels is also possible in the ECaTS system which provides additional comparative analysis opportunities within each reporting level (ex: compare PSAPs, or Counties).

Requirement: Ability to seamlessly report PSAP, ECD/County and State's 9-1-1 call statistics from one web-based location regardless of the CPE, Customer Premise Equipment, at the PSAPs.

The ECaTS system was designed as an agnostic reporting solution which can support all CPE vendors in the 911 industry. The system has been designed from the ground up to support any data stream and to normalize this stream into a common set of reportable parameters. ECaTS has a library that is constantly growing of ALI and CPE data parsing patterns that support all CPE currently present in the industry and can be easily expanded to those data formats that have yet to be encountered. ECaTS can provide demonstrations of reporting across multiple CPE's at the request of the State of Alabama.

Requirement: Ability to export reports in PDF, HTML, CVS and Excel formats

ECaTS provides exporting in all formats required: PDF, HTML, CSV, and Excel. In addition, the Excel export is configured to support older Excel 97' based system (with a 65,538 row limit) and current version of excel where the row limit exceeds one million rows. All reports in the ECaTS platform (Ad-hoc and standard) can be exported in the supported formats required by the State of Alabama. Exhibit 38 below shows the export options available in the ECATS standard and ad-hoc systems.



Standard Reports
- Call Summary
- Calls Per Hour
- Top Busiest Hours
- Average Call Duration
- Calls By Circuit
- Circuit Utilization
- PSAP Answer Time
- PSAP Call Taker Ring Time
- Last 12 Months Answer Time
- Last 12 Months Call Taker Ring Time
- Class of Service

REPORTS
No Report Selected

Select Psaps:
☐ Astoria 911
☐ Astoria 911 (Data Collector - A)
☐ Astoria 911 (Data Collector - B)
☐ Baker County Consolidated 911 Dispatch
☐ Brookings Police Department

OR

Select Group:
All
All PSAPs
Astoria 911
Astoria Data Collectors
Baker City Consolidated 911 Dispatch
Brookings Police Department
Bureau of Emergency Communications

☐ PSAP Grouping

Select Date Range: - SELECT -
From:
To:

Call Type: 911 Calls
Abandoned Filters: Include Abandoned

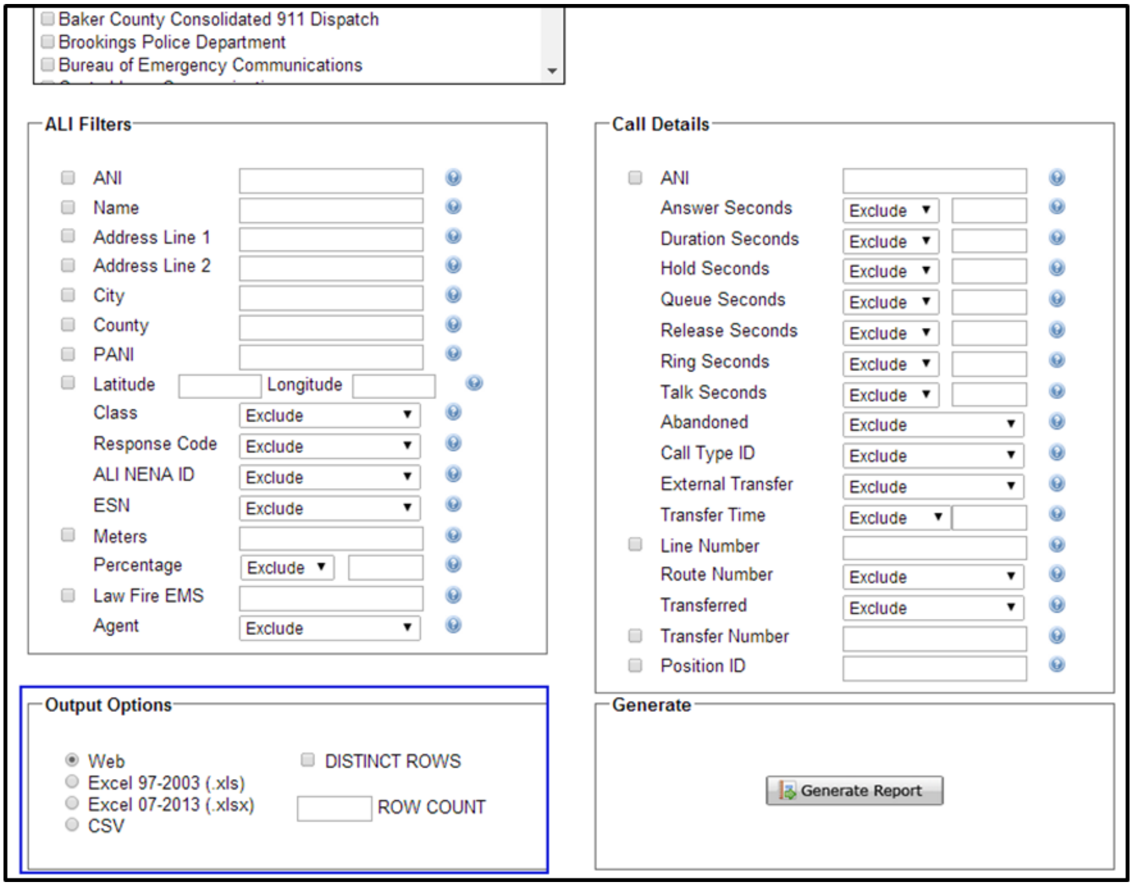
☐ Include Comparisons

Output Format: Web
Web
PDF
Excel

Graph Format: No Graph

ffiliation
☑ Fire ☑ Medical ☑ Military ☑ Police ☑ Sheriff ☑ University

Exhibit 38. Standard Reporting Output Options



□ Baker County Consolidated 911 Dispatch
□ Brookings Police Department
□ Bureau of Emergency Communications

ALI Filters

□	ANI	
□	Name	
□	Address Line 1	
□	Address Line 2	
□	City	
□	County	
□	PANI	
□	Latitude	Longitude
	Class	Exclude
	Response Code	Exclude
	ALI NENA ID	Exclude
	ESN	Exclude
□	Meters	
	Percentage	Exclude
□	Law Fire EMS	
	Agent	Exclude

Call Details

□	ANI	
	Answer Seconds	Exclude
	Duration Seconds	Exclude
	Hold Seconds	Exclude
	Queue Seconds	Exclude
	Release Seconds	Exclude
	Ring Seconds	Exclude
	Talk Seconds	Exclude
	Abandoned	Exclude
	Call Type ID	Exclude
	External Transfer	Exclude
	Transfer Time	Exclude
□	Line Number	
	Route Number	Exclude
	Transferred	Exclude
□	Transfer Number	
□	Position ID	

Output Options

● Web
○ Excel 97-2003 (.xls)
○ Excel 07-2013 (.xlsx)
○ CSV

□ DISTINCT ROWS

ROW COUNT

Generate

Requirement: Ability to generate universal reports from anywhere with an Internet connection and accessible on any devices with an internet browser, i.e. iPad, iPhones, iOS, Android or Windows based systems, laptops and desktops.

The ECaTS platform is a web based standards compliant MIS system. ECaTS only runs from a system that can load a browser either on a mobile (iOS, Android, Windows Phone) platform or a desktop platform (Windows, OS X, Linux) that can run a standards compliant browser (ex: Chrome, Firefox, Safari, IE). The MIS service itself is hosted at the ECaTS data center and if the State of Alabama allows, the access can be opened such that users can generate reports from any location with internet access vs. needing to be on a closed VPN connection from a State of Alabama network. The choice of open access vs. VPN is dependent on the security requirements and needs of the State of Alabama and ECaTS can accommodate any necessary model.

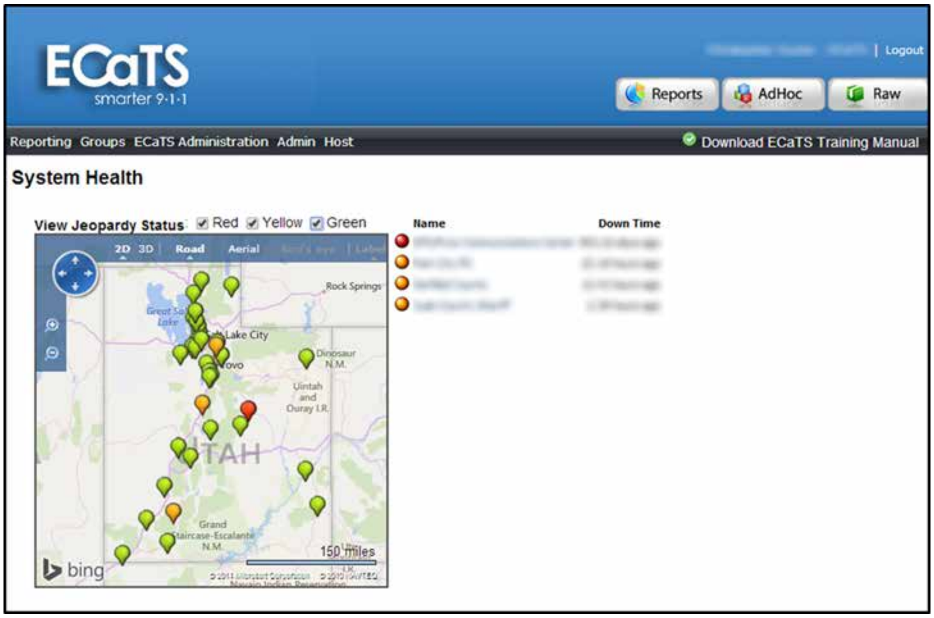
Requirement: Ability to analyze ANGEN's overall 911 system performance

As a system designed to provide multi-level reporting across multiple PSAPs the ability to analyze an entire statewide 911 deployment is as easy as reporting on all PSAPs in a single report. The ECaTS platform provides this level of reporting by combining data from the ESInet logger and the local PSAP CDR data. This enables a full end-to-end analysis of each call and of the 911 system itself. In addition to aggregating multiple data sources for a complete end-to end picture, ECaTS provides multiple means of grouping and sorting the data to ensure that the needed statewide information views are available and can generate the metrics required of the State of Alabama.

Requirement: Ability to provide a color coded map view of the State's System Health for all PSAPs in the State.

System Health

The ECaTS system provides a statewide view of all the PSAPs in Alabama using a map interface. Providing the Alabama 9-1-1 Board with a near real-time health monitoring system for all PSAPs that are covered by the ECaTS system. Each location is dynamically colored Green, Yellow or Red. This system health system monitors both the health and status of the RDDM collecting data at a particular PSAP and also performs real-time analytics and rendering of call volume and ALI bid activity. In the event call volume drops below historical moving averages a Low Call Volume alert (yellow) will occur bringing attention to the PSAP for call volume analysis. In addition to the call volume alerting, the system health also monitors for failed ALI bids and when concurrent failures for a single PSAP occur an alert (red) is created brining attention to the PSAP of a potential ALI bid issues. Exhibit 39 below illustrates system health for a statewide deployment.



System Health

View Jeopardy Status ☑ Red ☑ Yellow ☑ Green

Name	Down Time

Exhibit 39. System Health Interface

5.2.3 AD-HOC REPORTING SYSTEM

The system must provide the ability for ad-hoc reporting functionality:

The interface must provide drop-down list boxes, check boxes and other easy to use interface options for the selection and generation of ad-hoc reports.

The interface must provide users with access to all major fields in the system with help functions that clearly explain the value stored in each field.

The user must have the ability to save and share ad-hoc reports with other users in the system.

TCS Response: Comply.

Ad-Hoc Reports

Ad-Hoc reporting is one of the most powerful features of ECaTS and accessible through a user friendly interface. The Ad-Hoc functionality empowers authorized users with the ability to generate custom reports against any data element stored in the system, on the fly, with minimal computer skills.

Ad-Hoc Reports are aimed towards advanced users of ECaTS who demand flexibility from their reporting services. Users are able to enter three report screen formats: Standard, Advanced, and Shared. The Standard editor gives the user an easy method for choosing and applying filters by implementing intuitive drop down lists and checkboxes for each data element. The dropdown boxes dynamically change their content based on previously selected criteria to keep the interface simple. The Advanced editor enables the user to take Ad-Hoc reporting one step further by giving the user ability to integrate SQL style Boolean expressions.

This reporting tool enables the end user to comb through large amounts of data and give the user the ability to create a report that is specific to the user's needs. Our Ad-Hoc tool enables the end user to filter on specific fields from the ALI and CDR to build a customized output. Not only can Ad-Hoc reports be saved once they are defined, but they can also be shared with other ECaTS users.

To access the Ad-Hoc reporting tool select the 'Ad-Hoc' button from the top right hand side of the ECaTS portal screen shown in Exhibit 40.

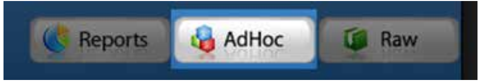
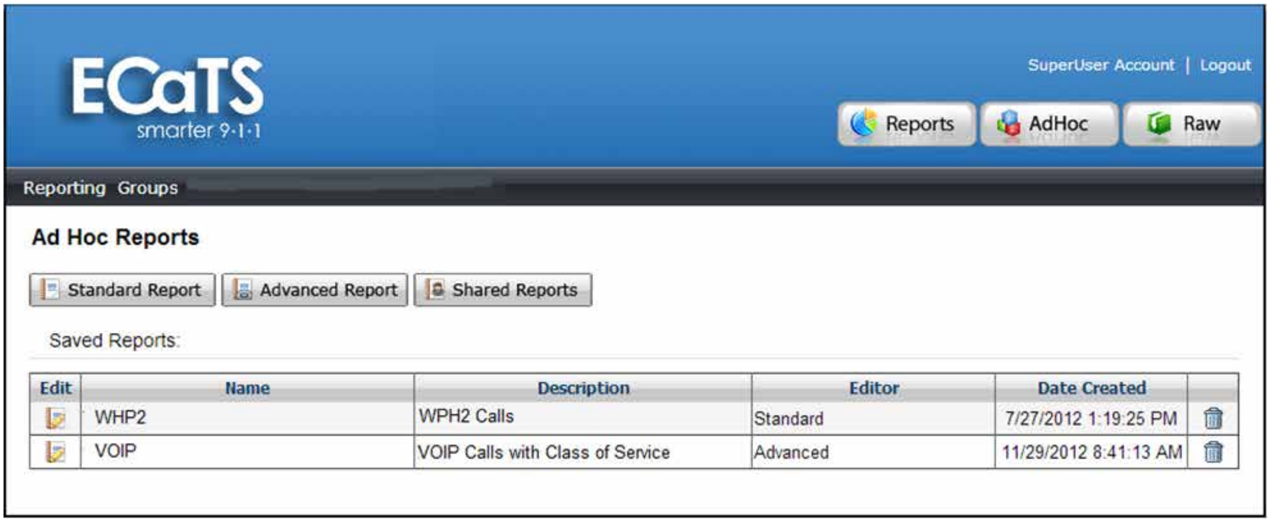


Exhibit 40. Ad Hoc Button on ECaTS Portal Screen

Ad-Hoc Homepage

By clicking on the Ad-Hoc button, ECaTS users will arrive at the Ad-Hoc home page. The homepage is a collection of the user's saved Ad-Hoc reports. Please note, there are three different types of Ad-Hoc reports: Standard Reports, Advanced Reports and Shared Reports. Standard and Advanced reports that are saved will be listed in the table on the following page.

The Ad-hoc Reporting system through the ECaTS portal allows each user to query the data based on user permissions and desired output. ECaTS features two Ad-hoc interfaces, Standard and Advanced.



ECaTS smarter 9-1-1

SuperUser Account | Logout

Reports AdHoc Raw

Reporting Groups

Ad Hoc Reports

Standard Report | Advanced Report | Shared Reports

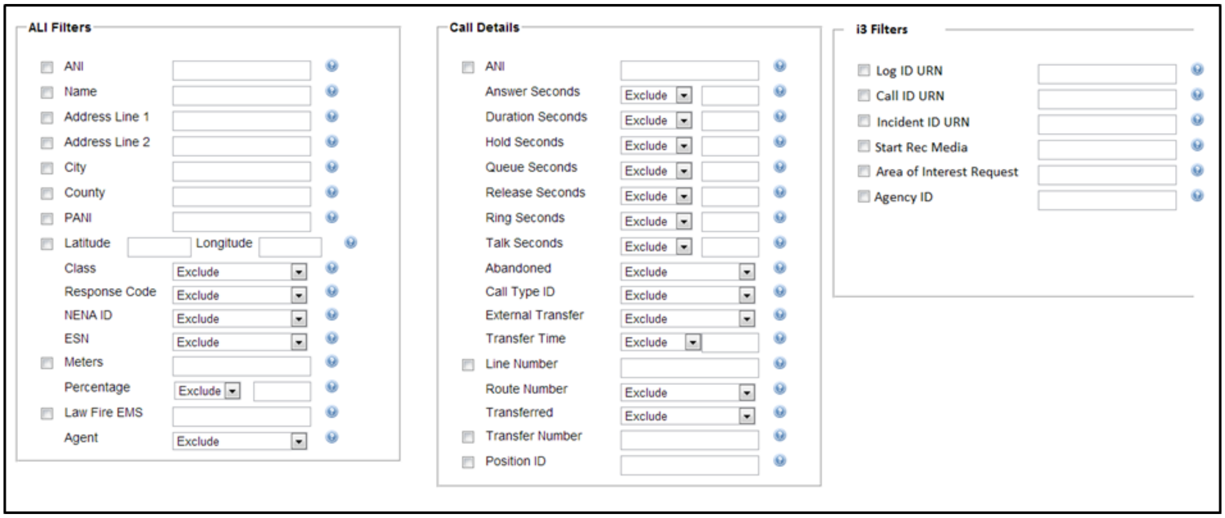
Saved Reports:

Edit	Name	Description	Editor	Date Created	
	WHP2	WPH2 Calls	Standard	7/27/2012 1:19:25 PM	
	VOIP	VOIP Calls with Class of Service	Advanced	11/29/2012 8:41:13 AM	

Exhibit 41. Ad-Hoc Homepage

Standard Ad-Hoc

Standard Ad-Hoc reporting is the most commonly used report generator. The search filters on the Standard viewer offer Boolean (true or false) expressions as well as distinct searches to find calls based on CDR and ALI information. As shown in Exhibit 42 below, there are three types of call data that a user can search on: ALI filters, Call Details and i3 Filters.



ALI Filters

- □ ANI
- □ Name
- □ Address Line 1
- □ Address Line 2
- □ City
- □ County
- □ PANI
- □ Latitude Longitude
- Class: Exclude
- Response Code: Exclude
- NENA ID: Exclude
- ESN: Exclude
- □ Meters
- Percentage: Exclude
- □ Law Fire EMS
- Agent: Exclude

Call Details

- □ ANI
- Answer Seconds: Exclude
- Duration Seconds: Exclude
- Hold Seconds: Exclude
- Queue Seconds: Exclude
- Release Seconds: Exclude
- Ring Seconds: Exclude
- Talk Seconds: Exclude
- Abandoned: Exclude
- Call Type ID: Exclude
- External Transfer: Exclude
- Transfer Time: Exclude
- □ Line Number
- Route Number: Exclude
- Transferred: Exclude
- □ Transfer Number
- □ Position ID

i3 Filters

- □ Log ID URN
- □ Call ID URN
- □ Incident ID URN
- □ Start Rec Media
- □ Area of Interest Request
- □ Agency ID

Exhibit 42. Standard Ad-Hoc Filters

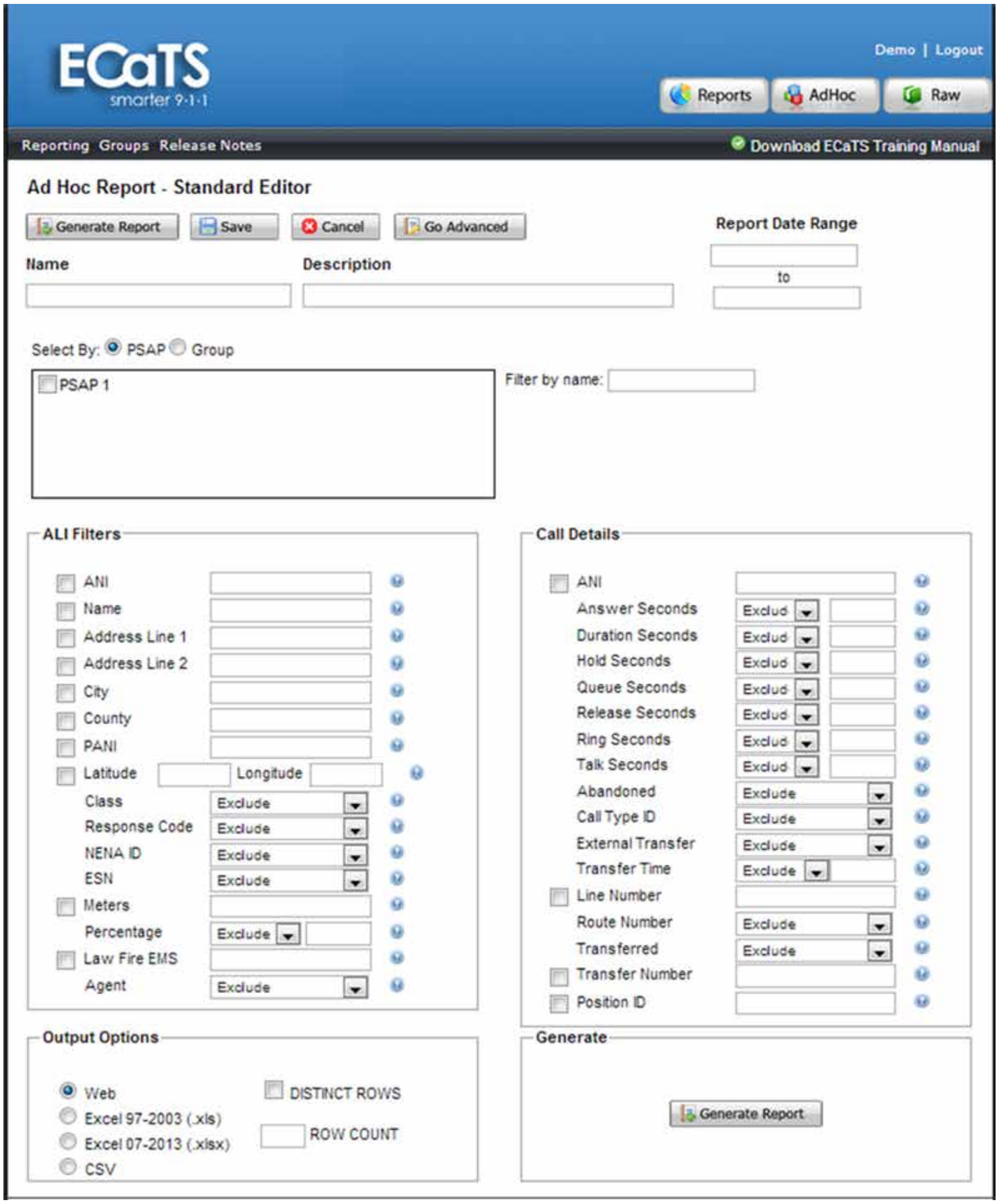
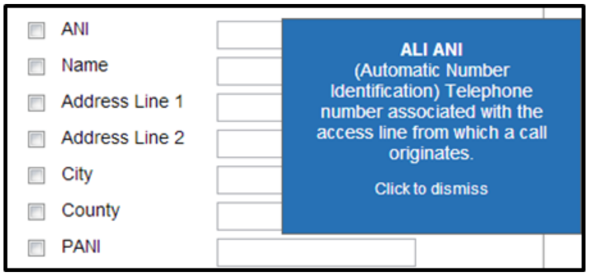


Exhibit 43. Standard Ad-Hoc Interface

Next to each of the fields' filters you will notice a blue '?' button that indicates what the field is used for. To better understand each field, click the '?' button for a description of the field, as shown in Exhibit 44 for "ANI".



□ ANI
□ Name
□ Address Line 1
□ Address Line 2
□ City
□ County
□ PANI

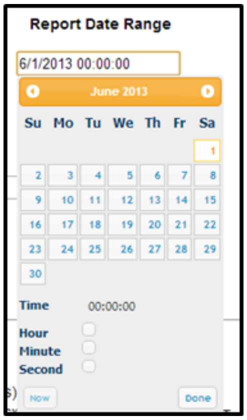
ALI ANI
(Automatic Number Identification) Telephone number associated with the access line from which a call originates.

Click to dismiss

Exhibit 44. Information Button for Each Filter Field

To search for partial or exact matches on a field, simply add what you are searching for in the text box and the search engine will do the rest. To include that search as an output column in the report, simply select the checkbox to the left of the field.

Ad-hoc also allows the user to narrow down reporting windows by hour, minute and second, offering the option to report by a specific shift or time/date range.



Report Date Range

6/1/2013 00:00:00

June 2013

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Time 00:00:00

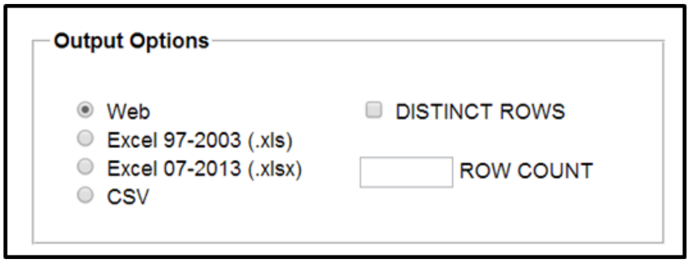
Hour □
Minute □
Second □

Now Done

Exhibit 45. Selecting Time Window for Report

Ad-hoc reporting provides multiple output format options. These options include:

1. Web
2. Excel 97-2003
3. Excel 2007-2013
4. CSV



Output Options

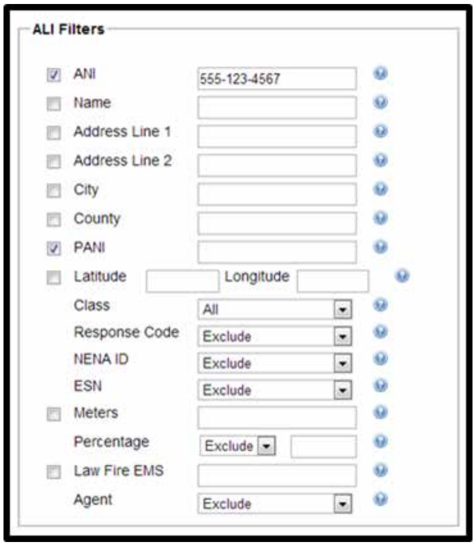
● Web
○ Excel 97-2003 (.xls)
○ Excel 07-2013 (.xlsx)
○ CSV

□ DISTINCT ROWS

ROW COUNT

Exhibit 46. Output Options

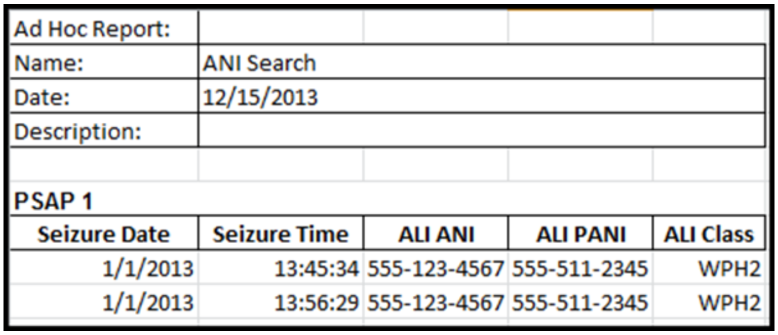
Standard Ad-hoc Report Example:



ALI Filters

☑ ANI 555-123-4567
□ Name
□ Address Line 1
□ Address Line 2
□ City
□ County
☑ PANI
□ Latitude Longitude
Class All
Response Code Exclude
NENA ID Exclude
ESN Exclude
□ Meters
Percentage Exclude
□ Law Fire EMS
Agent Exclude

Exhibit 47. Filters



Ad Hoc Report:				
Name:	ANI Search			
Date:	12/15/2013			
Description:				
PSAP 1				
Seizure Date	Seizure Time	ALI ANI	ALI PANI	ALI Class
1/1/2013	13:45:34	555-123-4567	555-511-2345	WPH2
1/1/2013	13:56:29	555-123-4567	555-511-2345	WPH2

Exhibit 48. Report Result (Excel Format)

Advanced Ad-Hoc

Advanced Ad-Hoc reporting is more often used by advanced or frequent ECaTS users. The search filters on the Advanced Ad-Hoc Viewer offer Boolean (true or false) expressions as well as distinct searches to find calls based on the source and fields selected.

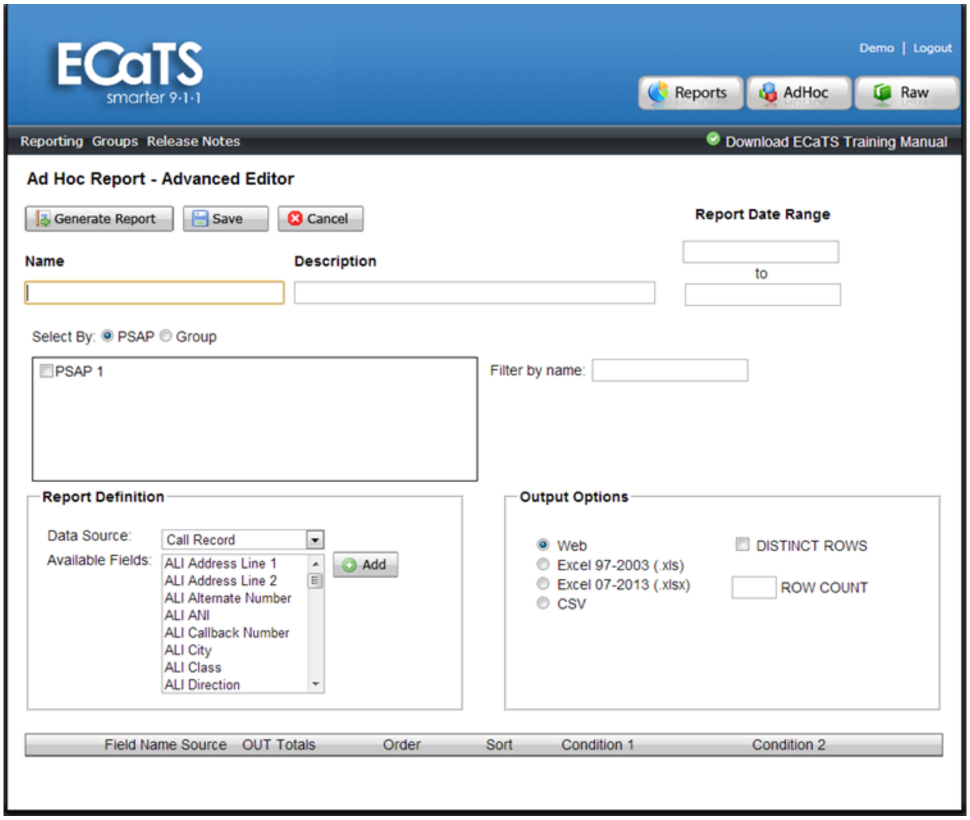
The Advanced Ad-hoc interface provides additional functionality for report building also using both CDR and ESInet meta data.

1. The user can choose the field to sort data by (in a descending or ascending order)
2. The user can choose the order of columns in the report
3. Totals may be selected per field, these totals include:
    - Count
    - Average
    - Min

- Max
- Sum

4. Multiple conditions per field may be entered

Advanced Ad-hoc Reporting Interface:



Ad Hoc Report - Advanced Editor

Report Date Range

to

Name

Description

Select By: ● PSAP ○ Group

□ PSAP 1

Filter by name:

Report Definition

Data Source: Call Record

Available Fields: ALI Address Line 1, ALI Address Line 2, ALI Alternate Number, ALI ANI, ALI Callback Number, ALI City, ALI Class, ALI Direction

Output Options

● Web
○ Excel 97-2003 (.xls)
○ Excel 07-2013 (.xlsx)
○ CSV

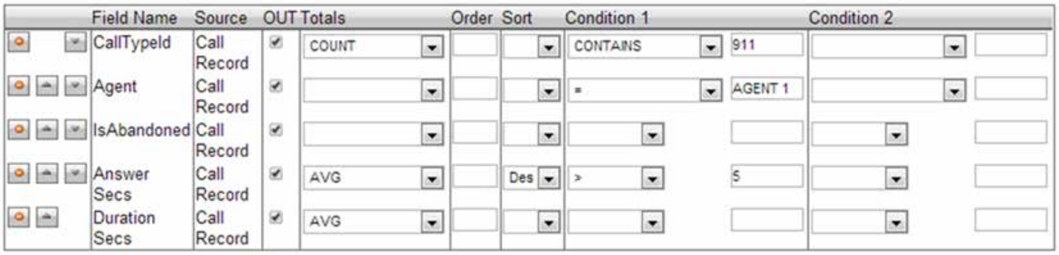
□ DISTINCT ROWS

ROW COUNT

Field Name	Source	OUT	Totals	Order	Sort	Condition 1	Condition 2

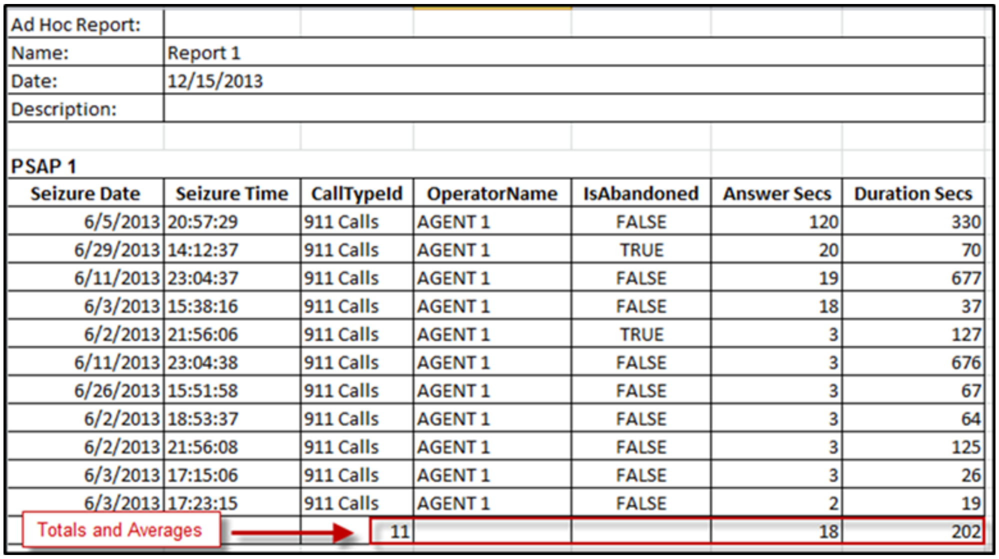
Exhibit 49. Advanced Ad-Hoc Interface

Advanced Ad-hoc Examples:



Field Name	Source	OUT	Totals	Order	Sort	Condition 1		Condition 2	
CallTypeId	Call Record	☑	COUNT			CONTAINS	911		
Agent	Call Record	☑				=	AGENT 1		
IsAbandoned	Call Record	☑							
Answer Secs	Call Record	☑	AVG		Des	>	5		
Duration Secs	Call Record	☑	AVG						

Exhibit 50. Report Filters



Ad Hoc Report:	
Name:	Report 1
Date:	12/15/2013
Description:	

PSAP 1

Seizure Date	Seizure Time	CallTypeId	OperatorName	IsAbandoned	Answer Secs	Duration Secs
6/5/2013	20:57:29	911 Calls	AGENT 1	FALSE	120	330
6/29/2013	14:12:37	911 Calls	AGENT 1	TRUE	20	70
6/11/2013	23:04:37	911 Calls	AGENT 1	FALSE	19	677
6/3/2013	15:38:16	911 Calls	AGENT 1	FALSE	18	37
6/2/2013	21:56:06	911 Calls	AGENT 1	TRUE	3	127
6/11/2013	23:04:38	911 Calls	AGENT 1	FALSE	3	676
6/26/2013	15:51:58	911 Calls	AGENT 1	FALSE	3	67
6/2/2013	18:53:37	911 Calls	AGENT 1	FALSE	3	64
6/2/2013	21:56:08	911 Calls	AGENT 1	FALSE	3	125
6/3/2013	17:15:06	911 Calls	AGENT 1	FALSE	3	26
6/3/2013	17:23:15	911 Calls	AGENT 1	FALSE	2	19
Totals and Averages		11			18	202

Exhibit 51. Report Results

Sharing Reports

ECaTS also allows authorized users to share reports generated in the ad-hoc reporting tool with other users of the application. For instance, a user may develop an ad-hoc report that yields specific or interesting analytics regarding 911 call volumes in their county or jurisdiction. They can then share the report with other authorized users so they may discuss the contents of the report or to provide additional insight into discussion topics for upcoming meetings.

5.2.4 SYSTEM DASHBOARD

The system shall provide a web based "Dashboard" that is based on User Role. Summary data on the Dashboard will provide "drill down" capabilities.

TCS Response: Comply.

ECaTS Real-Time Dashboard

ECaTS, Emergency Call Tracking System, Real-Time Dashboard is the first of its kind in the Public Safety Industry. The dashboard gives PSAP/County/State Management Personnel the ability to monitor 9-1-1 call activity in a visual real-time display.

The ECaTS Dashboard provides a visual representation of actual 911 call activity, answer time, hold time, and other factors, and clearly represents the real-or near-time condition of 9-1-1 within the specified jurisdiction. Additional analytics segment the data by wireless carrier providing a clear identification of wireless 9-1-1 calls or other communication data traffic through the PSAP/PSAPs in the State and/or County. Each data factor such as call volume will be compared against normative vales (averages) to identify anomalies in call traffic, call volume and call handling statistics. An area of the dashboard will be dedicated to mapping incoming calls to clearly illustrate possible areas of high traffic or anomalous call volume (either higher or lower than normal). Wireless carrier activity will also be compared against normative values and significant deviations between normal and abnormal call activity will be highlighted as an "alert" by the dashboard.

If additional functionality is desired of the real-time display, customizations can be done on a fixed bid basis after a joint application design session has been completed to determine the desired enhanced functionality.

Statewide/County/Individual PSAP Dashboard Display

ECaTS gives its users the ability to monitor real-time 9-1-1 call statistics Statewide, Countywide and at the individual PSAP. The Alabama 9-1-1 Board will have access to a live dashboard to assist in the following:

- Gathers of real-time intelligence and actionable information to enhance emergency response and public safety anywhere in the State.
- Combines big data/analytics technologies with real-time data feeds (i3 logging/ESInet) for improved interagency coordination and development of 'the right' resources.
- Ensures real-time situational awareness at both Local and State levels
- Enables enhanced early warning threat identification
- Supports faster inter-agency resource deployment at drastically reduced response times
- Offers, in some cases, the potential to proactively prevent loss of life, infrastructure or property.

Exhibit 52. Hanging State Dashboard Mockup

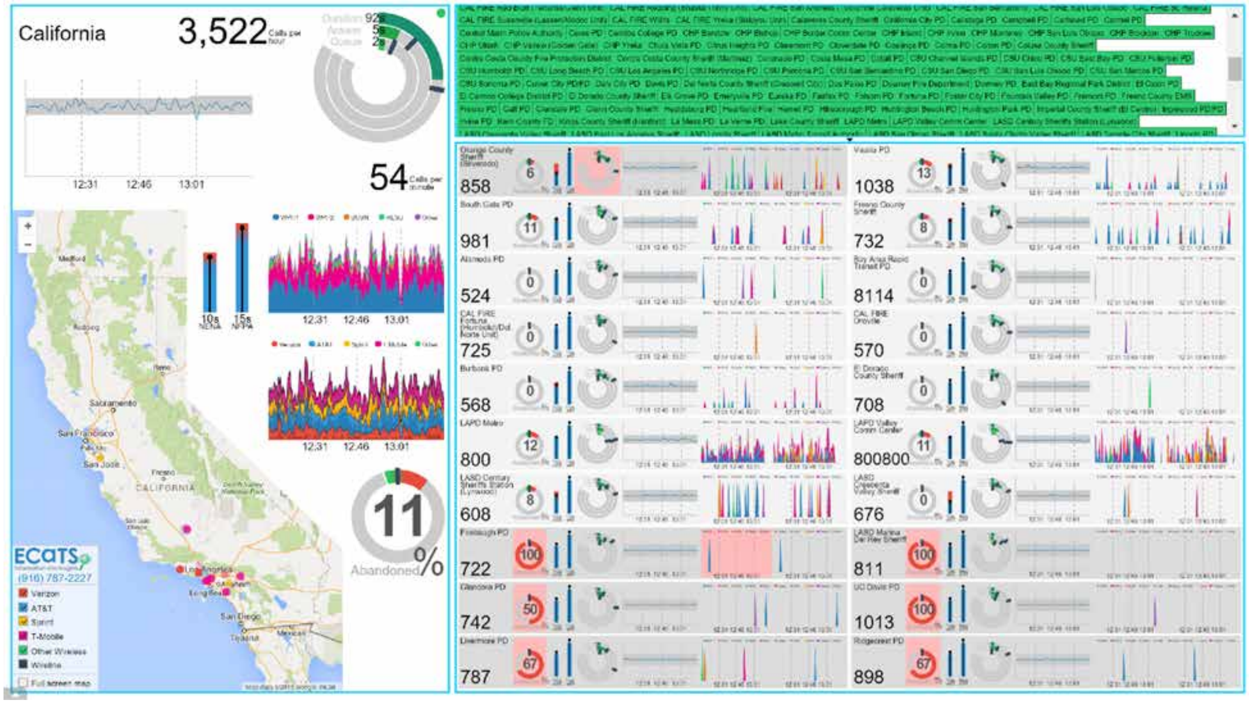


Exhibit 53. State Dashboard Overview

Exhibit 54 below shows a sample of the type of KPIs that can be monitored using the ECaTS Dashboard:

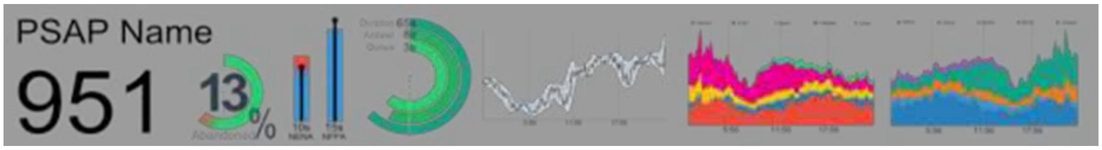
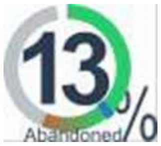
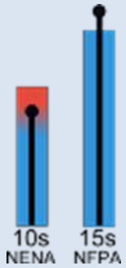
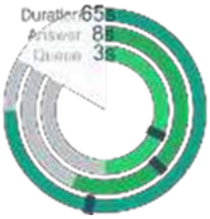
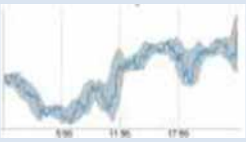
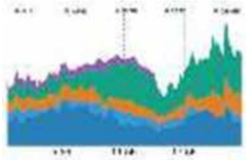
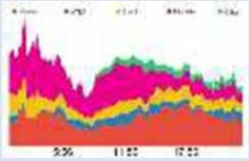


Exhibit 54. Dashboard Widgets

Exhibit 55. Dashboard Widgets Description

Field	Description
 PSAP Name 951	Represents the name of the PSAP and its FCC ID.
 13 Abandoned %	Represents the Abandoned call visualization for the PSAP as Changes: The abandoned percentage at the PSAP level is calculated over the past 60 minutes and updated every minute.

Field	Description
 	Represents the current answer time thresholds being met for both NENA and NFPA standards. Changes: The percentage of calls answered in less than 10 or 15 seconds at the PSAP level is calculated over the past 60 minutes and updated every minute.
 	Represents the current state of Duration, Answer Times and Queue times and any alerts for those timings. Changes: The current averages at the PSAP level are calculated over the past 60 minutes and updated every minute.
	Represents the PSAP call volume. Changes: Each data point at the PSAP level represents the number of calls in the past 60 minutes (calls per hour), updated every minute. The viewing window is the past hour with time labels at 15, 30, and 45 minutes in the past, precise to the minute.
	Represents the PSAP current class of service call volume. Changes: Call volume at the PSAP level is measured as the number of calls in the past 60 minutes, updated every minute. The viewing window is the past hour with time labels at 15, 30, and 45 minutes in the past, precise to the minute.
	Represents the PSAP current wireless carrier call volume. Changes: Call volume at the PSAP level is measured as the number of calls in the past 60 minutes, updated every minute. The viewing window is the past hour with time labels at 15, 30, and 45 minutes in the past, precise to the minute.

5.3 OPERATIONAL REPORTING AND LOGGING

The system shall provide access via Crystal Reports or a similar reporting tool to all data elements via a reporting server. Queries must be restricted to the reporting server which shall be as current or near real time as is practicable.

At a minimum, the following data elements shall be logged and readily available for reporting purposes at the system level and at the ECD/PSAP level:

- Payload processing times
- Answer time
- Disconnect time
- Incoming IP address
- Pre-Defined Reports – restricted to PSAP(s) based on user role
- Total count of Payloads by Type
- Average Event Waiting Report
- Average Event duration
- Total Abandoned Events
- Events by incoming IP address
- Events by hour of day
- Events answered by user ID
- Events by day of the week
- Events transferred
- Event transferred to PSAP
- Position answered
- Events answered by position
- Events answered by all positions
- Agent availability report
- Call volumes
- Individual Call detail Information
- Summary of Call Loads

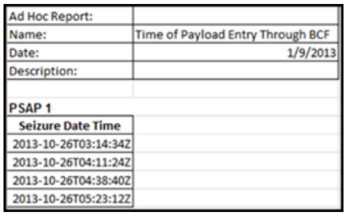
Respondents shall provide examples of operational reports and describe the ability of the system to capture, store and report on these data elements.

TCS Response: Comply.

The ECaTS reporting tool complies with all above-listed operational reporting and logging requirements. Below is a description of each.

Payload Processing Times

The payload processing time is calculated from the time the payload enters through the BCF until the call is routed to the PSAP via the ECRF.



Ad Hoc Report:	
Name:	Time of Payload Entry Through BCF
Date:	1/9/2013
Description:	

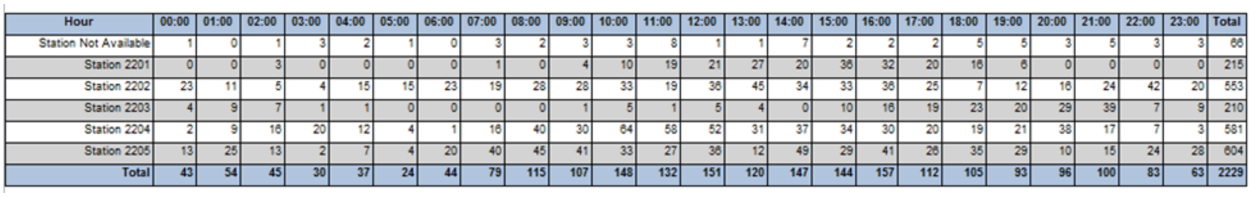
PSAP 1

Seizure Date Time
2013-10-26T03:14:34Z
2013-10-26T04:11:24Z
2013-10-26T04:38:40Z
2013-10-26T05:23:12Z

Exhibit 56. Payload Processing Times

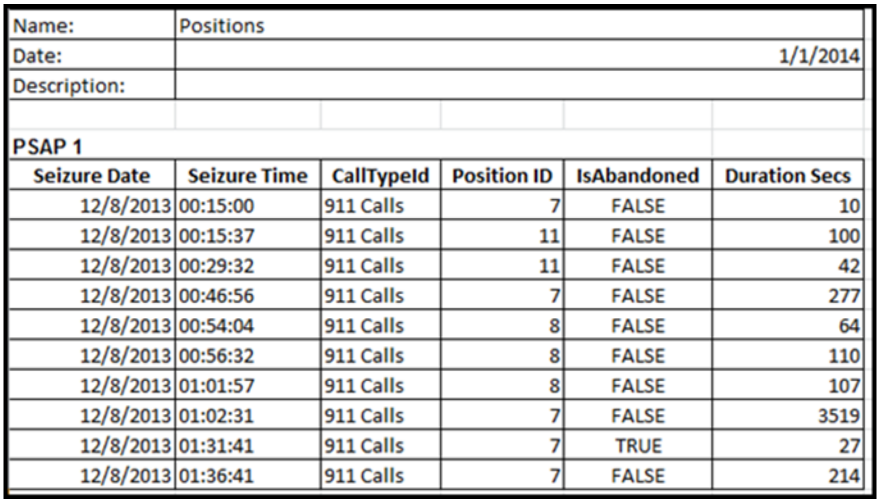
Position Answered

The position that answers each event will be recorded and reported on through the Initial Station Total Calls report. This report provides hourly counts for each answered event by position/station. In addition, the position that answered each event is a field in the ad-hoc system. A user has the ability to filter by position, or to simply include position number as a field in a report.



Hour	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	Total
Station Not Available	1	0	1	3	2	1	0	3	2	3	3	8	1	1	7	2	2	2	5	5	3	5	3	3	66
Station 2201	0	0	3	0	0	0	0	1	0	4	10	19	21	27	20	36	32	20	16	6	0	0	0	0	215
Station 2202	23	11	5	4	15	15	23	19	28	28	33	19	36	45	34	33	36	25	7	12	16	24	42	20	553
Station 2203	4	9	7	1	1	0	0	0	0	1	5	1	5	4	0	10	16	19	23	20	29	39	7	9	210
Station 2204	2	9	16	20	12	4	1	16	40	30	64	58	52	31	37	34	30	20	19	21	38	17	7	3	581
Station 2205	13	25	13	2	7	4	20	40	45	41	33	27	36	12	49	29	41	26	35	29	10	15	24	28	604
Total	**43**	**54**	**45**	**30**	**37**	**24**	**44**	**79**	**115**	**107**	**148**	**132**	**151**	**120**	**147**	**144**	**157**	**112**	**105**	**93**	**96**	**100**	**83**	**63**	**2229**

Exhibit 57. Initial Station Total Calls Report Example



Name:	Positions
Date:	1/1/2014
Description:	

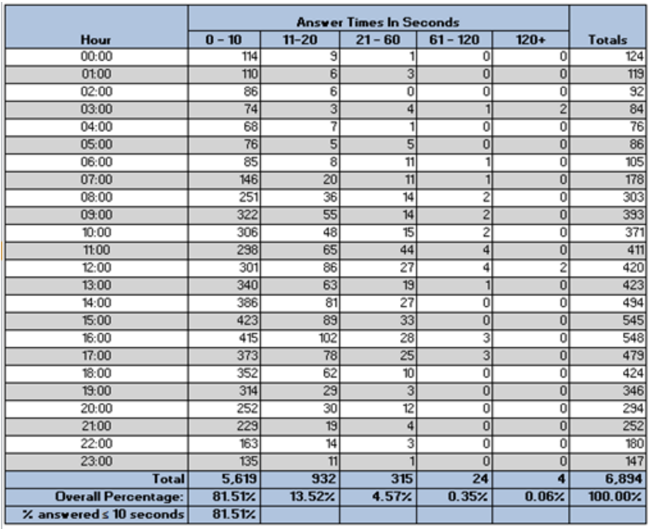
PSAP 1

Seizure Date	Seizure Time	CallTypeId	Position ID	IsAbandoned	Duration Secs
12/8/2013	00:15:00	911 Calls	7	FALSE	10
12/8/2013	00:15:37	911 Calls	11	FALSE	100
12/8/2013	00:29:32	911 Calls	11	FALSE	42
12/8/2013	00:46:56	911 Calls	7	FALSE	277
12/8/2013	00:54:04	911 Calls	8	FALSE	64
12/8/2013	00:56:32	911 Calls	8	FALSE	110
12/8/2013	01:01:57	911 Calls	8	FALSE	107
12/8/2013	01:02:31	911 Calls	7	FALSE	3519
12/8/2013	01:31:41	911 Calls	7	TRUE	27
12/8/2013	01:36:41	911 Calls	7	FALSE	214

Exhibit 58. Ad-Hoc Report Example

Answer Time

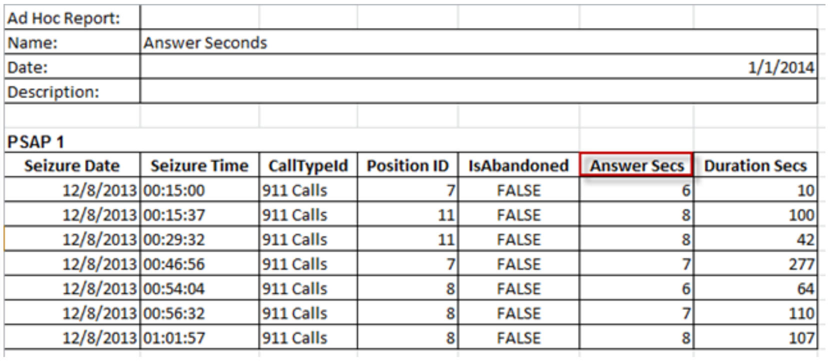
Answer time is calculated from seizure to event answer using the Call Handling supplied meta data. This is a field included on the Average Duration report, and is also used to create the PSAP Answer Time report.



Hour	Answer Times In Seconds					Totals
	0 - 10	11-20	21 - 60	61 - 120	120+	
00:00	114	9	1	0	0	124
01:00	110	6	3	0	0	119
02:00	86	6	0	0	0	92
03:00	74	3	4	1	2	84
04:00	68	7	1	0	0	76
05:00	76	5	5	0	0	86
06:00	85	8	11	1	0	105
07:00	146	20	11	1	0	178
08:00	251	36	14	2	0	303
09:00	322	55	14	2	0	393
10:00	306	48	15	2	0	371
11:00	298	65	44	4	0	411
12:00	301	86	27	4	2	420
13:00	340	63	19	1	0	423
14:00	386	81	27	0	0	494
15:00	423	89	33	0	0	545
16:00	415	102	28	3	0	548
17:00	373	78	25	3	0	479
18:00	352	62	10	0	0	424
19:00	314	29	3	0	0	346
20:00	252	30	12	0	0	294
21:00	229	19	4	0	0	252
22:00	163	14	3	0	0	180
23:00	135	11	1	0	0	147
Total	5,619	932	315	24	4	6,894
Overall Percentage:	81.51%	13.52%	4.57%	0.35%	0.06%	100.00%
% answered ≤ 10 seconds	81.51%					

Exhibit 59. Answer Time Report Example

In addition, answer seconds are a field available in ad-hoc. Users can include answer seconds, search by a specific range of answer seconds (such as <15 seconds), look at answer seconds for a specific position or operator, or build averages.



Ad Hoc Report:	
Name:	Answer Seconds
Date:	1/1/2014
Description:	

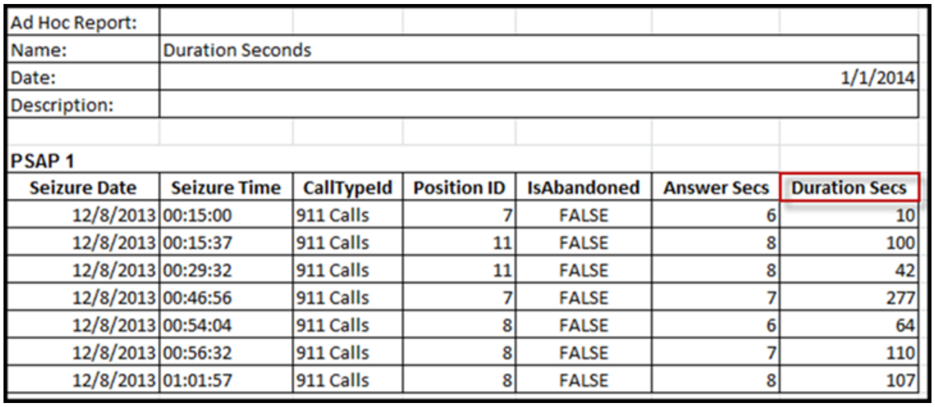
PSAP 1

Seizure Date	Seizure Time	CallTypeId	Position ID	IsAbandoned	Answer Secs	Duration Secs
12/8/2013	00:15:00	911 Calls	7	FALSE	6	10
12/8/2013	00:15:37	911 Calls	11	FALSE	8	100
12/8/2013	00:29:32	911 Calls	11	FALSE	8	42
12/8/2013	00:46:56	911 Calls	7	FALSE	7	277
12/8/2013	00:54:04	911 Calls	8	FALSE	6	64
12/8/2013	00:56:32	911 Calls	8	FALSE	7	110
12/8/2013	01:01:57	911 Calls	8	FALSE	8	107

Exhibit 60. Answer Seconds Field Available in Ad-Hoc Report

Disconnect Time

The disconnect time of a call is the total time of the call, which is also the duration value. ECaTS uses the duration as the disconnect time (or computed time value Time of call + Total duration of seconds) and these values can be found both in the Average Event Duration report or accessed as an ad hoc value as illustrated in Exhibit 61.



Ad Hoc Report:	
Name:	Duration Seconds
Date:	1/1/2014
Description:	

PSAP 1

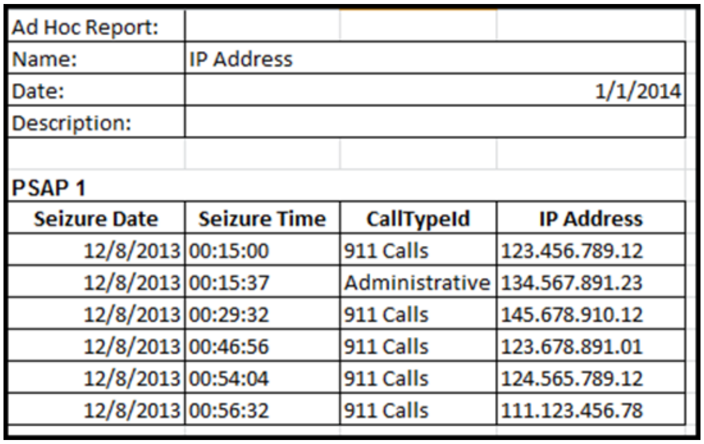
Seizure Date	Seizure Time	CallTypeId	Position ID	IsAbandoned	Answer Secs	Duration Secs
12/8/2013	00:15:00	911 Calls	7	FALSE	6	10
12/8/2013	00:15:37	911 Calls	11	FALSE	8	100
12/8/2013	00:29:32	911 Calls	11	FALSE	8	42
12/8/2013	00:46:56	911 Calls	7	FALSE	7	277
12/8/2013	00:54:04	911 Calls	8	FALSE	6	64
12/8/2013	00:56:32	911 Calls	8	FALSE	7	110
12/8/2013	01:01:57	911 Calls	8	FALSE	8	107

Exhibit 61. Disconnect Time

Incoming IP Address

The incoming IP address of each event will be stored as the field ‘Incoming IP Address’ and will be reportable through ad-hoc. This will allow the user to filter or search by a full or partial IP address. Users can build customized reports, including desired associated information.

In addition, the ‘Events by Incoming IP Address’ report will provide totals by incoming IP address for the date range selected (see Events by Incoming IP Address).



Ad Hoc Report:	
Name:	IP Address
Date:	1/1/2014
Description:	

PSAP 1

Seizure Date	Seizure Time	CallTypeId	IP Address
12/8/2013	00:15:00	911 Calls	123.456.789.12
12/8/2013	00:15:37	Administrative	134.567.891.23
12/8/2013	00:29:32	911 Calls	145.678.910.12
12/8/2013	00:46:56	911 Calls	123.678.891.01
12/8/2013	00:54:04	911 Calls	124.565.789.12
12/8/2013	00:56:32	911 Calls	111.123.456.78

Exhibit 62. Ad-Hoc Report Example

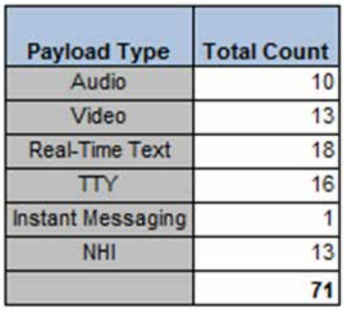
Total Count of Payloads by Type

Each event will include an indicator of payload ‘type’. The ‘Total Count of Payloads by Type’ report will provide total counts by payload type, and the overall number of payloads for the date range selected. The report may be customized to contain additional relevant/desired information.

Payload types are as follows:

1. Audio
2. Video
3. Real-Time Text
4. TTY (Baudout Tones)

5. Instant Messaging
6. NHI Events (Non-Human Initiated)

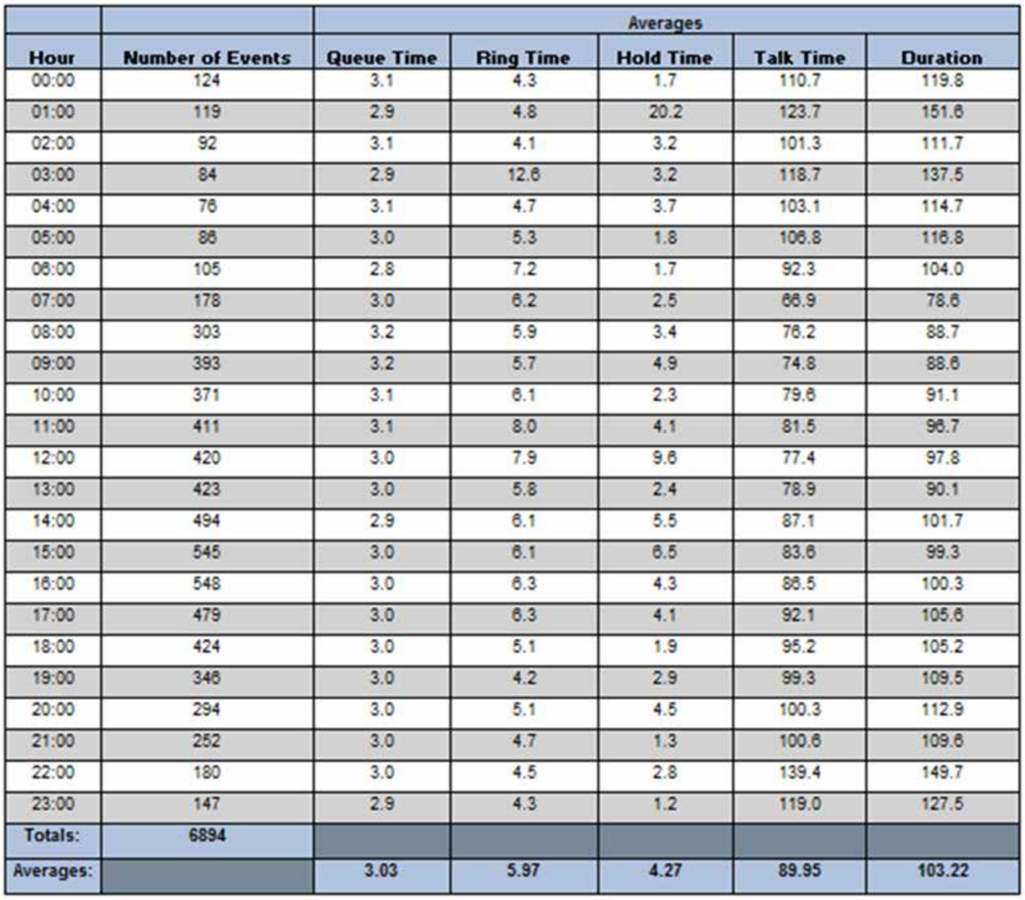


Payload Type	Total Count
Audio	10
Video	13
Real-Time Text	18
TTY	16
Instant Messaging	1
NHI	13
	71

Exhibit 63. Total Count by Payloads Type

Average Event Waiting Report

The average event waiting time can be obtained through the Average Duration report (as well as through ad-hoc).

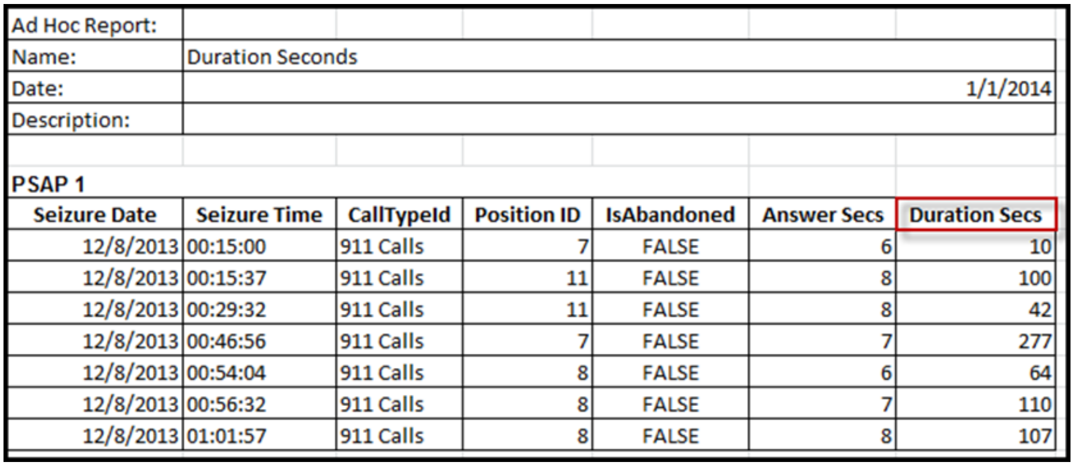


		Averages				
Hour	**Number of Events**	**Queue Time**	**Ring Time**	**Hold Time**	**Talk Time**	**Duration**
00:00	124	3.1	4.3	1.7	110.7	119.8
01:00	119	2.9	4.8	20.2	123.7	151.6
02:00	92	3.1	4.1	3.2	101.3	111.7
03:00	84	2.9	12.6	3.2	118.7	137.5
04:00	76	3.1	4.7	3.7	103.1	114.7
05:00	86	3.0	5.3	1.8	106.8	116.8
06:00	105	2.8	7.2	1.7	92.3	104.0
07:00	178	3.0	6.2	2.5	66.9	78.6
08:00	303	3.2	5.9	3.4	76.2	88.7
09:00	393	3.2	5.7	4.9	74.8	88.6
10:00	371	3.1	6.1	2.3	79.6	91.1
11:00	411	3.1	8.0	4.1	81.5	96.7
12:00	420	3.0	7.9	9.6	77.4	97.8
13:00	423	3.0	5.8	2.4	78.9	90.1
14:00	494	2.9	6.1	5.5	87.1	101.7
15:00	545	3.0	6.1	6.5	83.6	99.3
16:00	548	3.0	6.3	4.3	86.5	100.3
17:00	479	3.0	6.3	4.1	92.1	105.6
18:00	424	3.0	5.1	1.9	95.2	105.2
19:00	346	3.0	4.2	2.9	99.3	109.5
20:00	294	3.0	5.1	4.5	100.3	112.9
21:00	252	3.0	4.7	1.3	100.6	109.6
22:00	180	3.0	4.5	2.8	139.4	149.7
23:00	147	2.9	4.3	1.2	119.0	127.5
Totals:	**6894**					
Averages:		**3.03**	**5.97**	**4.27**	**89.95**	**103.22**

Exhibit 64. Average Event Waiting Report

Average Event Duration

The average duration will be located on the Average Duration report (see Average Event Waiting Time). In addition, duration seconds is a reportable field in ad-hoc and can be averaged and queried against based on parameters set by the user.

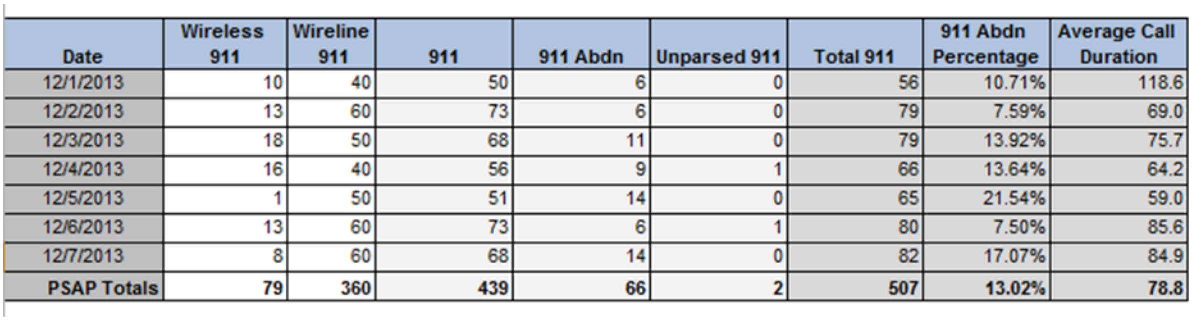


Ad Hoc Report:						
Name:	Duration Seconds					
Date:						1/1/2014
Description:						
PSAP 1						
Seizure Date	Seizure Time	CallTypeId	Position ID	IsAbandoned	Answer Secs	Duration Secs
12/8/2013	00:15:00	911 Calls	7	FALSE	6	10
12/8/2013	00:15:37	911 Calls	11	FALSE	8	100
12/8/2013	00:29:32	911 Calls	11	FALSE	8	42
12/8/2013	00:46:56	911 Calls	7	FALSE	7	277
12/8/2013	00:54:04	911 Calls	8	FALSE	6	64
12/8/2013	00:56:32	911 Calls	8	FALSE	7	110
12/8/2013	01:01:57	911 Calls	8	FALSE	8	107

Exhibit 65. Average Event Duration Ad-Hoc Report

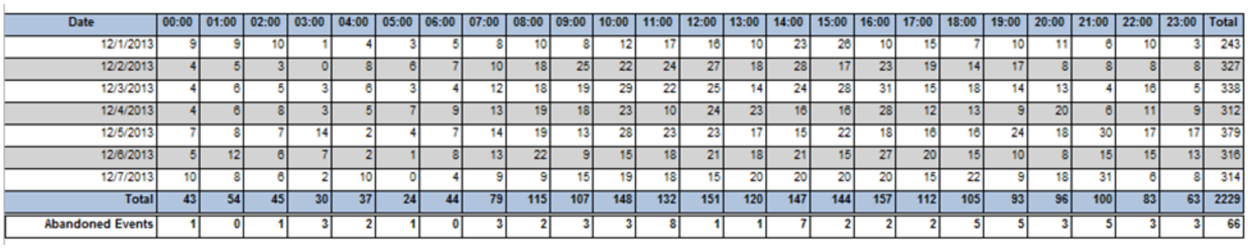
Total Abandoned Events

The Event Summary report will provide summary information regarding events, such as the number of events answered, the number of events abandoned, and the percentage of abandoned events. The Event Summary can be ran on each type of event individually, or all event types.



Date	Wireless 911	Wireline 911	911	911 Abdn	Unparsed 911	Total 911	911 Abdn Percentage	Average Call Duration
12/1/2013	10	40	50	6	0	56	10.71%	118.6
12/2/2013	13	60	73	6	0	79	7.59%	69.0
12/3/2013	18	50	68	11	0	79	13.92%	75.7
12/4/2013	16	40	56	9	1	66	13.64%	64.2
12/5/2013	1	50	51	14	0	65	21.54%	59.0
12/6/2013	13	60	73	6	1	80	7.50%	85.6
12/7/2013	8	60	68	14	0	82	17.07%	84.9
PSAP Totals	**79**	**360**	**439**	**66**	**2**	**507**	**13.02%**	**78.8**

Exhibit 66. Event Summary Report

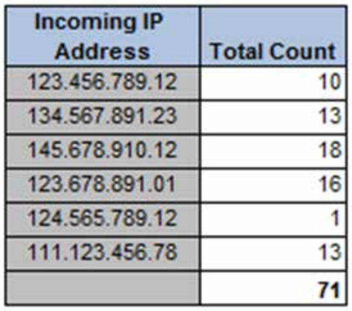


Date	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	Total
12/1/2013	9	9	10	1	4	3	5	8	10	8	12	17	16	10	23	26	10	15	7	10	11	6	10	3	243
12/2/2013	4	5	3	0	8	6	7	10	18	25	22	24	27	18	28	17	23	19	14	17	8	8	8	8	327
12/3/2013	4	6	5	3	6	3	4	12	18	19	29	22	25	14	24	28	31	15	18	14	13	4	16	5	338
12/4/2013	4	6	8	3	5	7	9	13	19	18	23	10	24	23	16	16	28	12	13	9	20	6	11	9	312
12/5/2013	7	8	7	14	2	4	7	14	19	13	28	23	23	17	15	22	18	16	16	24	18	30	17	17	379
12/6/2013	5	12	6	7	2	1	8	13	22	9	15	18	21	18	21	15	27	20	15	10	8	15	15	13	316
12/7/2013	10	8	6	2	10	0	4	9	9	15	19	18	15	20	20	20	20	15	22	9	18	31	6	8	314
Total	**43**	**54**	**45**	**30**	**37**	**24**	**44**	**79**	**115**	**107**	**148**	**132**	**151**	**120**	**147**	**144**	**157**	**112**	**105**	**93**	**96**	**100**	**83**	**63**	**2229**
Abandoned Events	1	0	1	3	2	1	0	3	2	3	3	8	1	1	7	2	2	2	5	5	3	5	3	3	66

Exhibit 67. Abandoned Events Per Hour

Events by Incoming IP Address

The ‘Events by Incoming IP Address’ report will provide total counts by IP address for the date range selected. Once selecting the ‘Events by IP Address’ report in the parameters screen, the user will be presented with checkboxes used to select the event(s) included in the report. The report may be customized to include additional relevant or desired information.



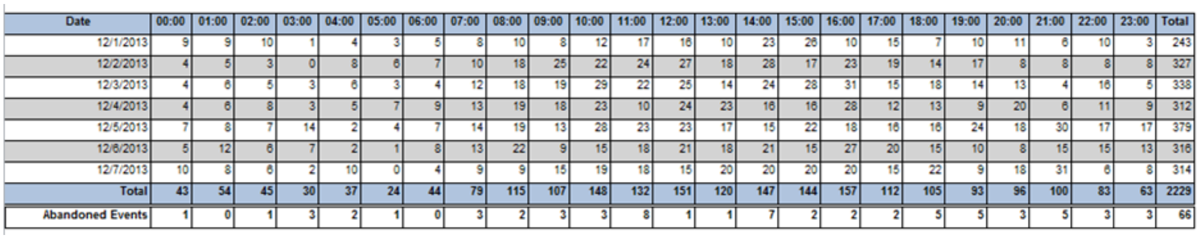
Incoming IP Address	Total Count
123.456.789.12	10
134.567.891.23	13
145.678.910.12	18
123.678.891.01	16
124.565.789.12	1
111.123.456.78	13
	71

Exhibit 68. Events by Incoming IP Address

Events by Hour of Day

The Events per Hour report will provide event counts by hour of day. The hour the event is placed in will be determined by the seizure time of the event. Once selecting the ‘Events per Hour’ report in the parameters screen, the user will be presented with checkboxes used to select the event(s) included in the report. Some examples of available events are:

1. Audio
2. Video
3. Real-Time Text Messaging
4. Instant Messaging
5. TTY

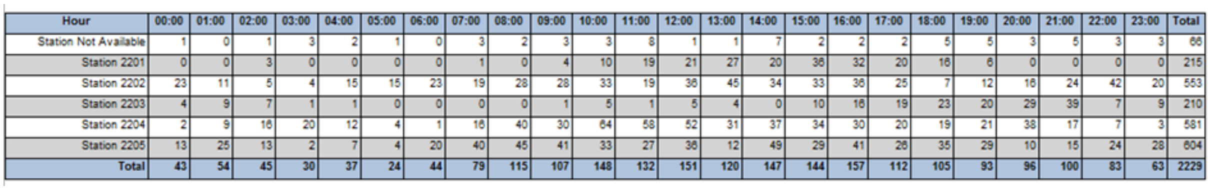


Date	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	Total
12/1/2013	9	9	10	1	4	3	5	8	10	8	12	17	16	10	23	26	10	15	7	10	11	6	10	3	243
12/2/2013	4	5	3	0	8	6	7	10	18	25	22	24	27	18	28	17	23	19	14	17	8	8	8	8	327
12/3/2013	4	6	5	3	6	3	4	12	18	19	29	22	25	14	24	28	31	15	18	14	13	4	16	5	338
12/4/2013	4	6	8	3	5	7	9	13	19	18	23	10	24	23	16	16	28	12	13	9	20	6	11	9	312
12/5/2013	7	8	7	14	2	4	7	14	19	13	28	23	23	17	15	22	18	16	16	24	18	30	17	17	379
12/6/2013	5	12	6	7	2	1	8	13	22	9	15	18	21	18	21	15	27	20	15	10	8	15	15	13	316
12/7/2013	10	8	6	2	10	0	4	9	9	15	19	18	15	20	20	20	20	15	22	9	18	31	6	8	314
Total	43	54	45	30	37	24	44	79	115	107	148	132	151	120	147	144	157	112	105	93	96	100	83	63	2229
Abandoned Events	1	0	1	3	2	1	0	3	2	3	3	8	1	1	7	2	2	2	5	5	3	5	3	3	66

Exhibit 69. Events Per Hour Report Example

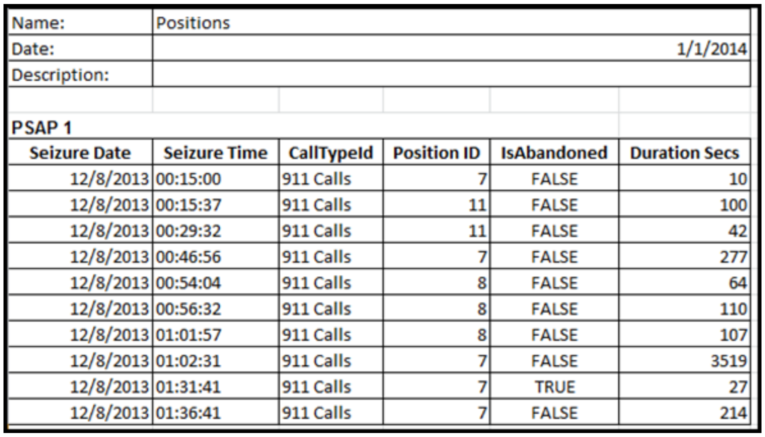
Events Answered by Position

The position that answers each event will be recorded and reported on through the Initial Station Total Events report. This report provides hourly counts for each answered event by position/station.



Hour	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	Total
Station Not Available	1	0	1	3	2	1	0	3	2	3	3	8	1	1	7	2	2	2	5	5	3	5	3	3	66
Station 2201	0	0	3	0	0	0	0	1	0	4	10	19	21	27	20	36	32	20	16	6	0	0	0	0	215
Station 2202	23	11	5	4	15	15	23	19	28	28	33	19	36	45	34	33	36	25	7	12	16	24	42	20	553
Station 2203	4	9	7	1	1	0	0	0	0	1	5	1	5	4	0	10	16	19	23	20	29	39	7	9	210
Station 2204	2	9	16	20	12	4	1	16	40	30	64	58	52	31	37	34	30	20	19	21	38	17	7	3	581
Station 2205	13	25	13	2	7	4	20	40	45	41	33	27	36	12	49	29	41	26	35	29	10	15	24	28	604
Total	43	54	45	30	37	24	44	79	115	107	148	132	151	120	147	144	157	112	105	93	96	100	83	63	2229

Exhibit 70. Initial Station Total Events Report Example



Name:	Positions				
Date:	1/1/2014				
Description:					
PSAP 1					
Seizure Date	Seizure Time	CallTypeId	Position ID	IsAbandoned	Duration Secs
12/8/2013	00:15:00	911 Calls	7	FALSE	10
12/8/2013	00:15:37	911 Calls	11	FALSE	100
12/8/2013	00:29:32	911 Calls	11	FALSE	42
12/8/2013	00:46:56	911 Calls	7	FALSE	277
12/8/2013	00:54:04	911 Calls	8	FALSE	64
12/8/2013	00:56:32	911 Calls	8	FALSE	110
12/8/2013	01:01:57	911 Calls	8	FALSE	107
12/8/2013	01:02:31	911 Calls	7	FALSE	3519
12/8/2013	01:31:41	911 Calls	7	TRUE	27
12/8/2013	01:36:41	911 Calls	7	FALSE	214

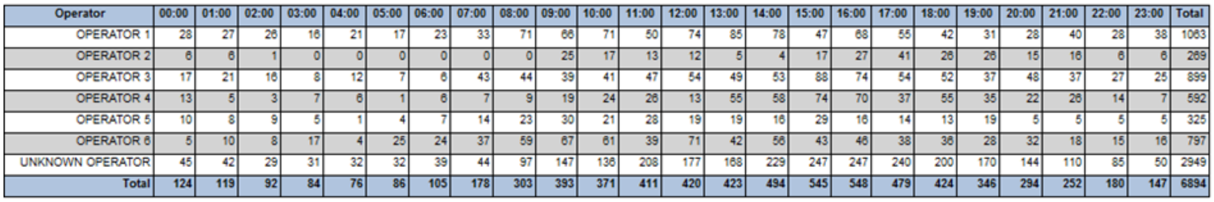
Exhibit 71. Ad-Hoc Report Example

Events Answered by All Positions

The events answered by all positions requirement will be fulfilled by use of the Event Summary report. This report will provide overall information regarding the number of events answered (regardless of position). If a user desires to look at all events answered across all stations, the Initial Station Total Events report will fulfill this need (see above).

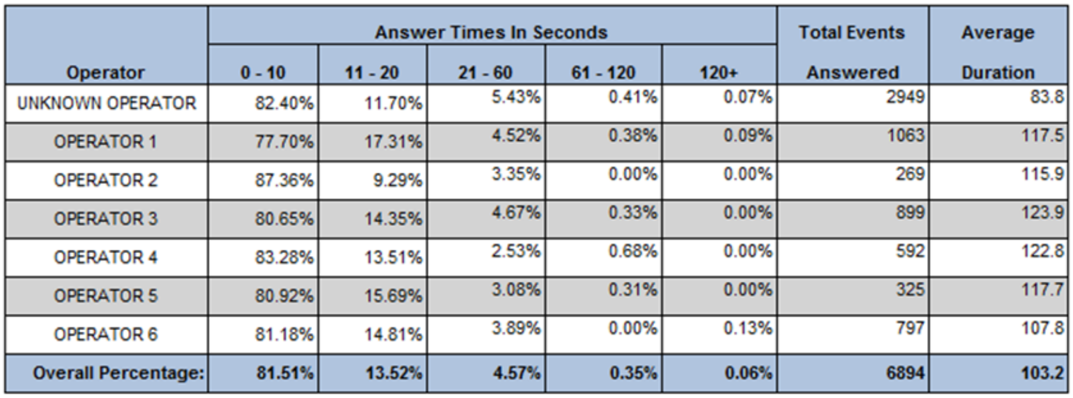
Events Answered by User ID

If each operator uses a unique user ID, the user ID will be stored as ‘Agent’ and can be reported against in multiple ways. ‘Agent’ is an available ad-hoc field, the user can query against answer time by operator, by a specific shift, etc. In addition, operator reports are available such as ‘Events by Operator’ and ‘Operator Speed of Answer’. These reports provide the number of events answered by each initial operator.



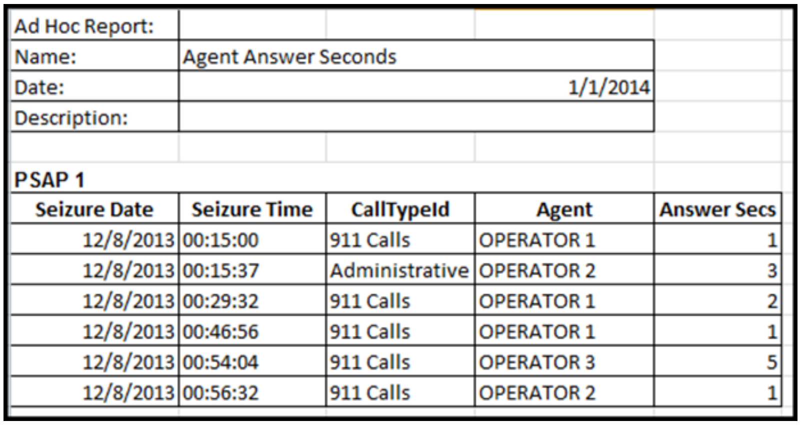
Operator	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	Total
OPERATOR 1	28	27	26	16	21	17	23	33	71	66	71	50	74	85	78	47	68	55	42	31	28	40	28	38	1063
OPERATOR 2	6	6	1	0	0	0	0	0	0	25	17	13	12	5	4	17	27	41	26	26	15	16	6	6	269
OPERATOR 3	17	21	16	8	12	7	6	43	44	39	41	47	54	49	53	88	74	54	52	37	48	37	27	25	899
OPERATOR 4	13	5	3	7	6	1	6	7	9	19	24	26	13	55	58	74	70	37	55	35	22	26	14	7	592
OPERATOR 5	10	8	9	5	1	4	7	14	23	30	21	28	19	19	16	29	16	14	13	19	5	5	5	5	325
OPERATOR 6	5	10	8	17	4	25	24	37	59	67	61	39	71	42	56	43	46	38	36	28	32	18	15	16	797
UNKNOWN OPERATOR	45	42	29	31	32	32	39	44	97	147	136	208	177	168	229	247	247	240	200	170	144	110	85	50	2949
Total	124	119	92	84	76	86	105	178	303	393	371	411	420	423	494	545	548	479	424	346	294	252	180	147	6894

Exhibit 72. Events by Operator Report Example



Operator	Answer Times In Seconds					Total Events	Average
	0 - 10	11 - 20	21 - 60	61 - 120	120+	Answered	Duration
UNKNOWN OPERATOR	82.40%	11.70%	5.43%	0.41%	0.07%	2949	83.8
OPERATOR 1	77.70%	17.31%	4.52%	0.38%	0.09%	1063	117.5
OPERATOR 2	87.36%	9.29%	3.35%	0.00%	0.00%	269	115.9
OPERATOR 3	80.65%	14.35%	4.67%	0.33%	0.00%	899	123.9
OPERATOR 4	83.28%	13.51%	2.53%	0.68%	0.00%	592	122.8
OPERATOR 5	80.92%	15.69%	3.08%	0.31%	0.00%	325	117.7
OPERATOR 6	81.18%	14.81%	3.89%	0.00%	0.13%	797	107.8
Overall Percentage:	**81.51%**	**13.52%**	**4.57%**	**0.35%**	**0.06%**	**6894**	**103.2**

Exhibit 73. Operator Speed of Answer Report Example



Ad Hoc Report:	
Name:	Agent Answer Seconds
Date:	1/1/2014
Description:	

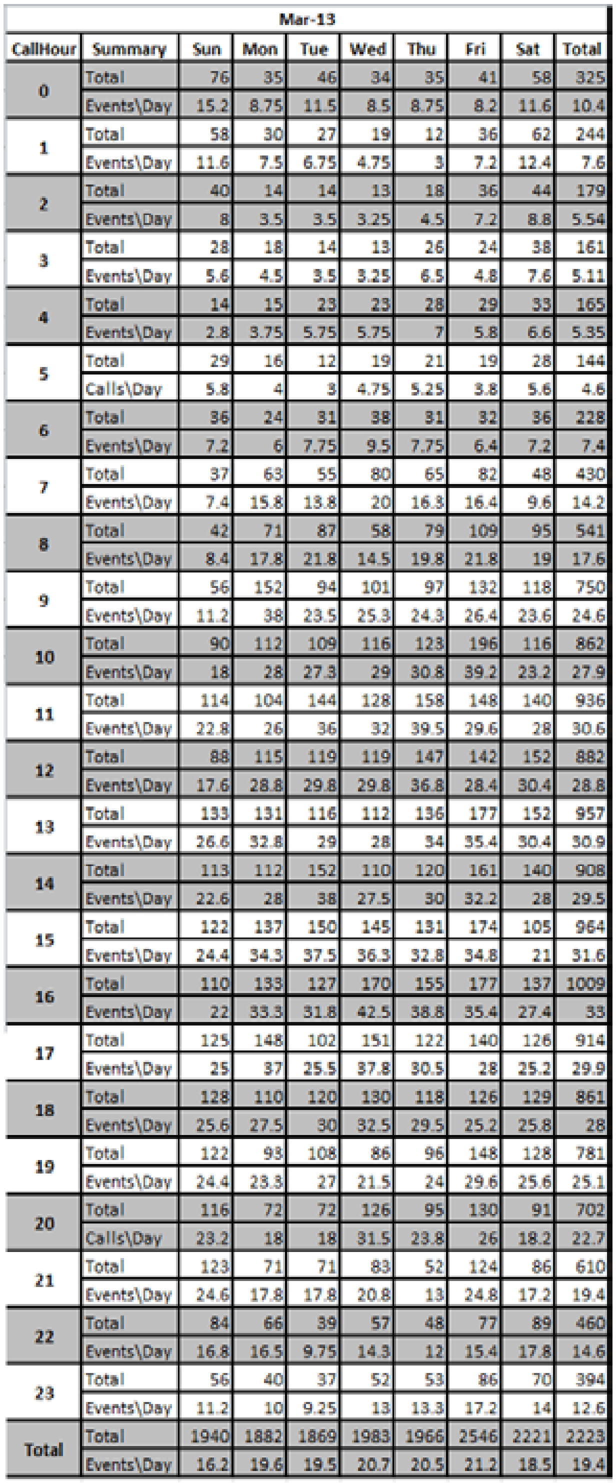
PSAP 1

Seizure Date	Seizure Time	CallTypeId	Agent	Answer Secs
12/8/2013	00:15:00	911 Calls	OPERATOR 1	1
12/8/2013	00:15:37	Administrative	OPERATOR 2	3
12/8/2013	00:29:32	911 Calls	OPERATOR 1	2
12/8/2013	00:46:56	911 Calls	OPERATOR 1	1
12/8/2013	00:54:04	911 Calls	OPERATOR 3	5
12/8/2013	00:56:32	911 Calls	OPERATOR 2	1

Exhibit 74. Ad-Hoc Report Example

Events by Day of the Week

Event reporting by day of week is available through the Events per Hour by Day of Week report. This report provides event counts by day of week as well as by hour of day.



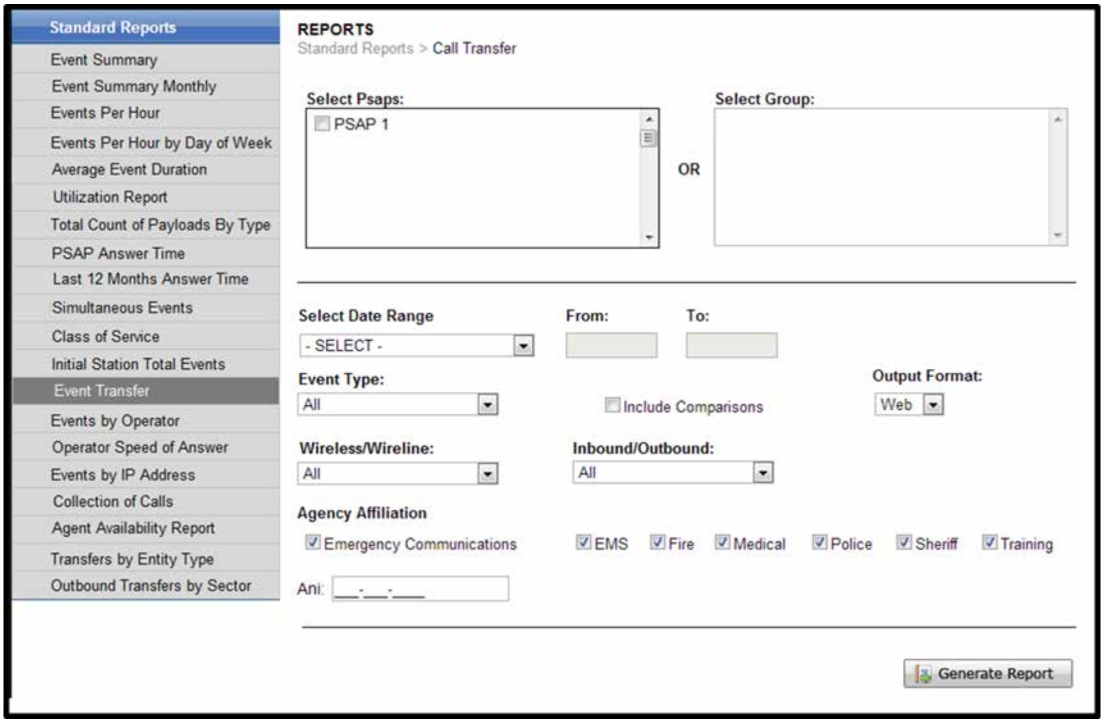
Mar-13									
CallHour	Summary	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Total
0	Total	76	35	46	34	35	41	58	325
	Events\Day	15.2	8.75	11.5	8.5	8.75	8.2	11.6	10.4
1	Total	58	30	27	19	12	36	62	244
	Events\Day	11.6	7.5	6.75	4.75	3	7.2	12.4	7.6
2	Total	40	14	14	13	18	36	44	179
	Events\Day	8	3.5	3.5	3.25	4.5	7.2	8.8	5.54
3	Total	28	18	14	13	26	24	38	161
	Events\Day	5.6	4.5	3.5	3.25	6.5	4.8	7.6	5.11
4	Total	14	15	23	23	28	29	33	165
	Events\Day	2.8	3.75	5.75	5.75	7	5.8	6.6	5.35
5	Total	29	16	12	19	21	19	28	144
	Calls\Day	5.8	4	3	4.75	5.25	3.8	5.6	4.6
6	Total	36	24	31	38	31	32	36	228
	Events\Day	7.2	6	7.75	9.5	7.75	6.4	7.2	7.4
7	Total	37	63	55	80	65	82	48	430
	Events\Day	7.4	15.8	13.8	20	16.3	16.4	9.6	14.2
8	Total	42	71	87	58	79	109	95	541
	Events\Day	8.4	17.8	21.8	14.5	19.8	21.8	19	17.6
9	Total	56	152	94	101	97	132	118	750
	Events\Day	11.2	38	23.5	25.3	24.3	26.4	23.6	24.6
10	Total	90	112	109	116	123	196	116	862
	Events\Day	18	28	27.3	29	30.8	39.2	23.2	27.9
11	Total	114	104	144	128	158	148	140	936
	Events\Day	22.8	26	36	32	39.5	29.6	28	30.6
12	Total	88	115	119	119	147	142	152	882
	Events\Day	17.6	28.8	29.8	29.8	36.8	28.4	30.4	28.8
13	Total	133	131	116	112	136	177	152	957
	Events\Day	26.6	32.8	29	28	34	35.4	30.4	30.9
14	Total	113	112	152	110	120	161	140	908
	Events\Day	22.6	28	38	27.5	30	32.2	28	29.5
15	Total	122	137	150	145	131	174	105	964
	Events\Day	24.4	34.3	37.5	36.3	32.8	34.8	21	31.6
16	Total	110	133	127	170	155	177	137	1009
	Events\Day	22	33.3	31.8	42.5	38.8	35.4	27.4	33
17	Total	125	148	102	151	122	140	126	914
	Events\Day	25	37	25.5	37.8	30.5	28	25.2	29.9
18	Total	128	110	120	130	118	126	129	861
	Events\Day	25.6	27.5	30	32.5	29.5	25.2	25.8	28
19	Total	122	93	108	86	96	148	128	781
	Events\Day	24.4	23.3	27	21.5	24	29.6	25.6	25.1
20	Total	116	72	72	126	95	130	91	702
	Calls\Day	23.2	18	18	31.5	23.8	26	18.2	22.7
21	Total	123	71	71	83	52	124	86	610
	Events\Day	24.6	17.8	17.8	20.8	13	24.8	17.2	19.4
22	Total	84	66	39	57	48	77	89	460
	Events\Day	16.8	16.5	9.75	14.3	12	15.4	17.8	14.6
23	Total	56	40	37	52	53	86	70	394
	Events\Day	11.2	10	9.25	13	13.3	17.2	14	12.6
Total	Total	1940	1882	1869	1983	1966	2546	2221	2223
	Events\Day	16.2	19.6	19.5	20.7	20.5	21.2	18.5	19.4

Exhibit 75. Events per Hour by Day of Week Report Example

Events Transferred

Transferred events can be reported against in a variety of ways. The first is the Event Transfer report. The parameters interface for the ‘Events Transferred’ report will also feature a filtering option for ‘Wireless’ and ‘Wireline’ transfers.

The report interface will also feature a drop-down menu with three transfer options, ‘All’, ‘Inbound’ and ‘Outbound.’



REPORTS
Standard Reports > Call Transfer

Select Psaps: □ PSAP 1
OR
Select Group:

Select Date Range: - SELECT -
From:
To:

Event Type: All
□ Include Comparisons
Output Format: Web

Wireless/Wireline: All
Inbound/Outbound: All

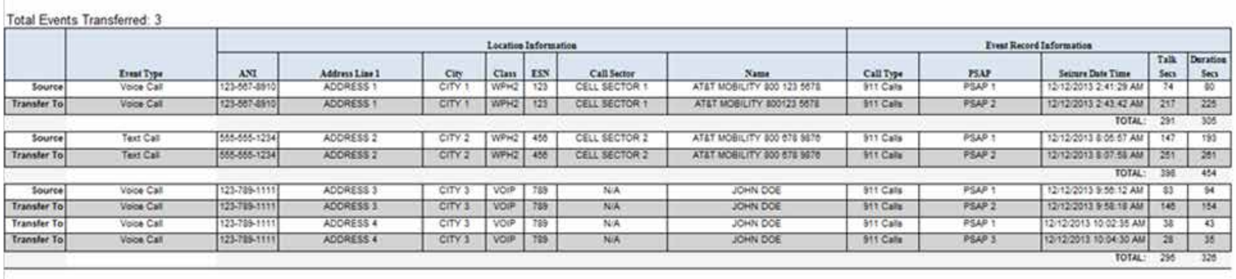
Agency Affiliation
☑ Emergency Communications ☑ EMS ☑ Fire ☑ Medical ☑ Police ☑ Sheriff ☑ Training

Ani: ___-___-____

Exhibit 76. Report Interface with Drop-Down Menus

Necessary associated information such as location or class of service will be included, as well as seizure time at each PSAP and the duration at each PSAP. The Event Transfer report can be filtered by ANI to easily locate a specific event.

If an event is transferred multiple times, the chaining will be apparent in the report. As displayed below, a call with multiple transfers will appear as a chain with each row representing an appearance of that event at each PSAP.

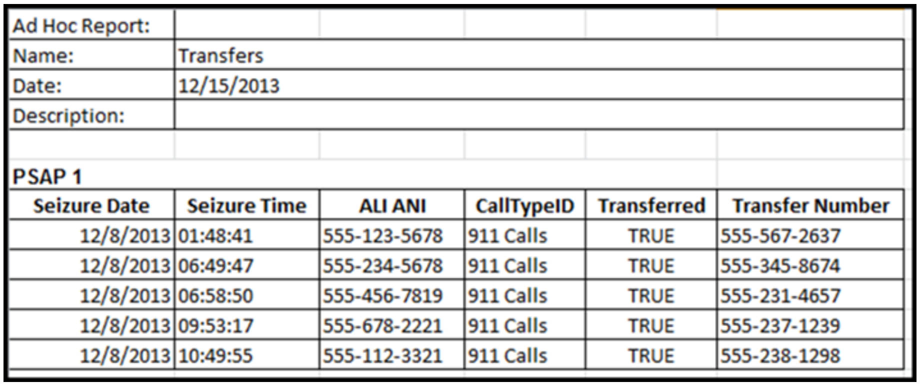


Total Events Transferred: 3

		Location Information							Event Record Information				
	Event Type	ANI	Address Line 1	City	Class	ESN	Call Sector	Name	Call Type	PSAP	Seizure Date Time	Talk Secs	Duration Secs
Source	Voice Call	123-567-8910	ADDRESS 1	CITY 1	WPH2	123	CELL SECTOR 1	AT&T MOBILITY 800 123 5678	911 Calls	PSAP 1	12/12/2013 2:41:29 AM	74	80
Transfer To	Voice Call	123-567-8910	ADDRESS 1	CITY 1	WPH2	123	CELL SECTOR 1	AT&T MOBILITY 800123 5678	911 Calls	PSAP 2	12/12/2013 2:43:42 AM	217	225
											TOTAL:	291	305
Source	Text Call	555-555-1234	ADDRESS 2	CITY 2	WPH2	456	CELL SECTOR 2	AT&T MOBILITY 800 678 9876	911 Calls	PSAP 1	12/12/2013 8:05:57 AM	147	193
Transfer To	Text Call	555-555-1234	ADDRESS 2	CITY 2	WPH2	456	CELL SECTOR 2	AT&T MOBILITY 800 678 9876	911 Calls	PSAP 2	12/12/2013 8:07:58 AM	251	261
											TOTAL:	398	454
Source	Voice Call	123-789-1111	ADDRESS 3	CITY 3	VOIP	789	N/A	JOHN DOE	911 Calls	PSAP 1	12/12/2013 9:56:12 AM	83	94
Transfer To	Voice Call	123-789-1111	ADDRESS 3	CITY 3	VOIP	789	N/A	JOHN DOE	911 Calls	PSAP 2	12/12/2013 9:58:18 AM	146	154
Transfer To	Voice Call	123-789-1111	ADDRESS 4	CITY 3	VOIP	789	N/A	JOHN DOE	911 Calls	PSAP 1	12/12/2013 10:02:35 AM	38	43
Transfer To	Voice Call	123-789-1111	ADDRESS 4	CITY 3	VOIP	789	N/A	JOHN DOE	911 Calls	PSAP 3	12/12/2013 10:04:30 AM	28	35
											TOTAL:	296	326

Exhibit 77. Calls with Multiple Transfers Appearing as Chain

In addition, transfer counts can be obtained through ad-hoc with the ‘Transferred’ field. Dialed transfer numbers will be stored for reporting purposes; this will allow any user to determine transfer counts to any outside entity through ad-hoc.



Ad Hoc Report:	
Name:	Transfers
Date:	12/15/2013
Description:	

PSAP 1

Seizure Date	Seizure Time	ALI ANI	CallTypeID	Transferred	Transfer Number
12/8/2013	01:48:41	555-123-5678	911 Calls	TRUE	555-567-2637
12/8/2013	06:49:47	555-234-5678	911 Calls	TRUE	555-345-8674
12/8/2013	06:58:50	555-456-7819	911 Calls	TRUE	555-231-4657
12/8/2013	09:53:17	555-678-2221	911 Calls	TRUE	555-237-1239
12/8/2013	10:49:55	555-112-3321	911 Calls	TRUE	555-238-1298

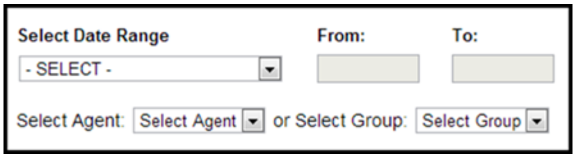
Exhibit 78. Ad-Hoc Report Showing Transferred Calls

Agent Availability Report

The Agent Availability Report provides information on each operator. Once selecting the ‘Agent Availability Report’ in the parameters screen, the user can select one or more operators (agents) to be included in the report.

Users will have the ability to build Agent Groups. These groups may contain one or more operators of the user’s choice. An unlimited number of groups can be built (for example, to address each shift). The report includes for the entire specified date range:

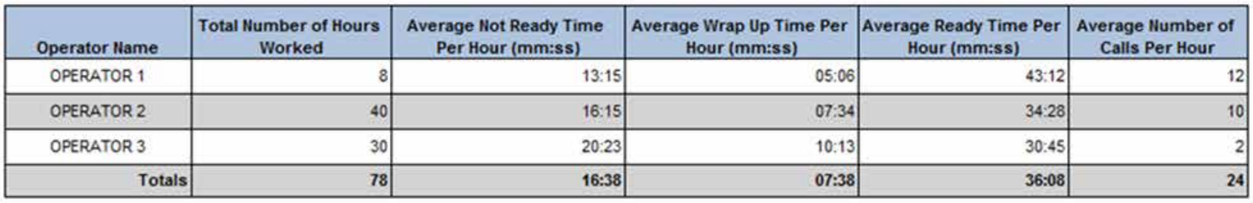
1. The number of total hours worked
2. Average Not Ready time per hour (mm:ss format)
3. Average Wrap Up time per hour (mm:ss)
4. Average Ready (Idle) Time per hour (mm:ss)
5. Average Number of Calls per hour



Select Date Range: - SELECT - ▾ From: To:

Select Agent: Select Agent ▾ or Select Group: Select Group ▾

Exhibit 79. Report Parameters Example



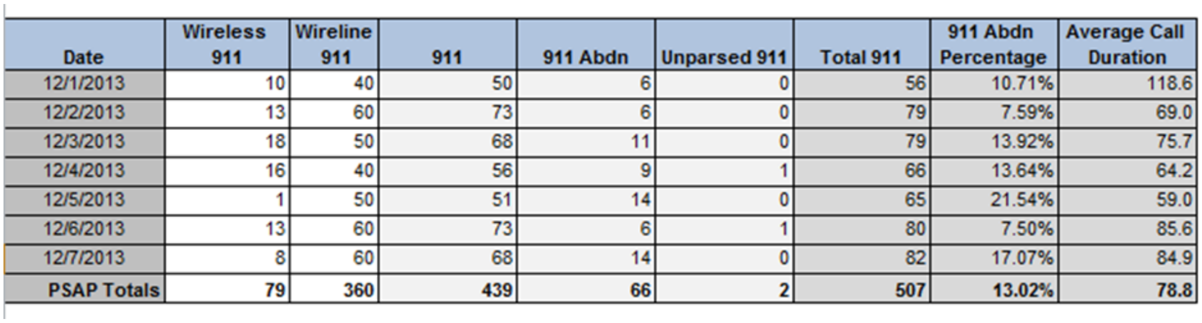
Operator Name	Total Number of Hours Worked	Average Not Ready Time Per Hour (mm:ss)	Average Wrap Up Time Per Hour (mm:ss)	Average Ready Time Per Hour (mm:ss)	Average Number of Calls Per Hour
OPERATOR 1	8	13:15	05:06	43:12	12
OPERATOR 2	40	16:15	07:34	34:28	10
OPERATOR 3	30	20:23	10:13	30:45	2
Totals	**78**	**16:38**	**07:38**	**36:08**	**24**

Exhibit 80. Agent Availability Report Example

Call Volumes

911, 10-Digit Emergency and Administrative call volume can be obtained in a single report, the Event Summary Report. The user will select the report, select ‘call’ as the Event Type, and then will be presented with call type options for the report. The Event Summary report contains wireless 911 and wireline 911 call counts, abandoned call counts, outbound call counts, overall totals and average call duration.

The event type (and all other parameters selected) will be listed in the report header, as depicted in Exhibit 81:

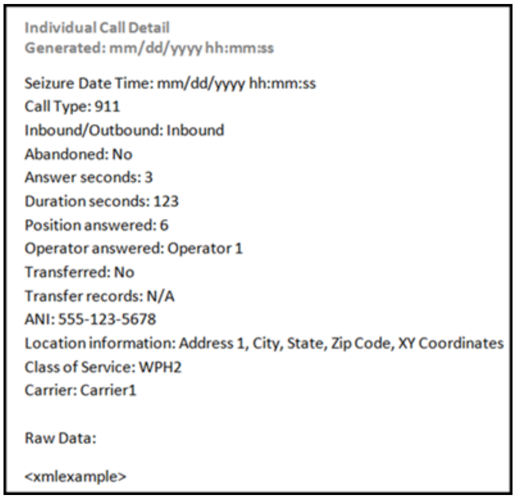


Date	Wireless 911	Wireline 911	911	911 Abdn	Unparsed 911	Total 911	911 Abdn Percentage	Average Call Duration
12/1/2013	10	40	50	6	0	56	10.71%	118.6
12/2/2013	13	60	73	6	0	79	7.59%	69.0
12/3/2013	18	50	68	11	0	79	13.92%	75.7
12/4/2013	16	40	56	9	1	66	13.64%	64.2
12/5/2013	1	50	51	14	0	65	21.54%	59.0
12/6/2013	13	60	73	6	1	80	7.50%	85.6
12/7/2013	8	60	68	14	0	82	17.07%	84.9
PSAP Totals	**79**	**360**	**439**	**66**	**2**	**507**	**13.02%**	**78.8**

Exhibit 81. Event Summary Report

Individual Call Information

Each call and its associated information can be obtained through the ad-hoc system. The user can query by using specific filters, or by including all information in the report. In this way, the user can obtain thorough information on each individual call.



Individual Call Detail
Generated: mm/dd/yyyy hh:mm:ss

Seizure Date Time: mm/dd/yyyy hh:mm:ss
Call Type: 911
Inbound/Outbound: Inbound
Abandoned: No
Answer seconds: 3
Duration seconds: 123
Position answered: 6
Operator answered: Operator 1
Transferred: No
Transfer records: N/A
ANI: 555-123-5678
Location information: Address 1, City, State, Zip Code, XY Coordinates
Class of Service: WPH2
Carrier: Carrier1

Raw Data:

<xmlexample>

Exhibit 82. Individual Call Detail

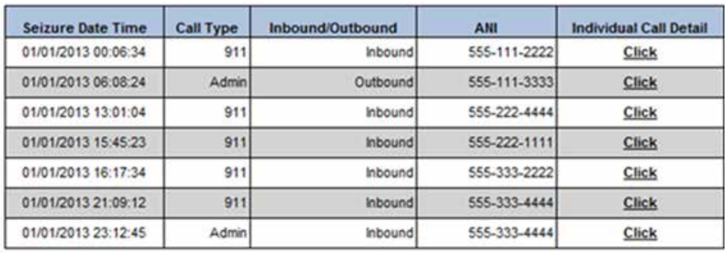
In addition, after generating the ‘Drill-Down’ report, a user may click a call on the report. Upon clicking the desired call, an ‘Individual Call Information’ report will open in a new window.

Collection of Calls

This report will provide call detail on all calls for the date range selected. The report detail will include:

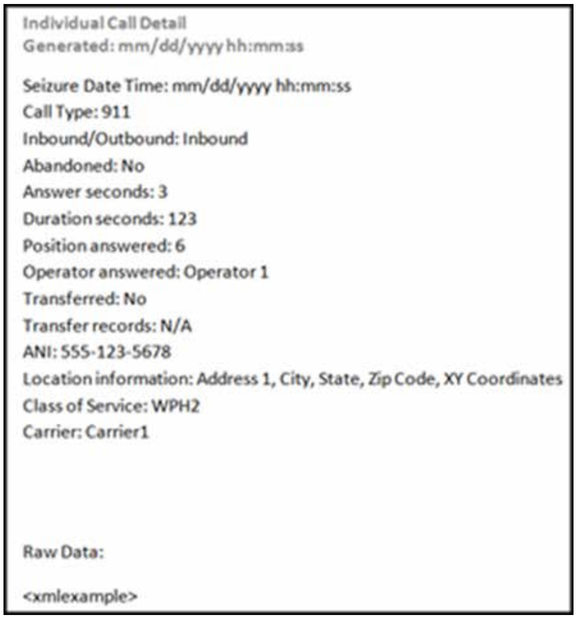
1. Seizure Time
2. Call Type
3. Inbound/Outbound
4. ANI

Once the report is generated, and calls have populated in the report, the user then has the ability to click on each report in the list. Clicking into a particular call will open a new report with individual call detail. This 'Individual Call Detail' report will provide all information associated with the call, including the raw XML data.



Seizure Date Time	Call Type	Inbound/Outbound	ANI	Individual Call Detail
01/01/2013 00:06:34	911	Inbound	555-111-2222	Click
01/01/2013 06:08:24	Admin	Outbound	555-111-3333	Click
01/01/2013 13:01:04	911	Inbound	555-222-4444	Click
01/01/2013 15:45:23	911	Inbound	555-222-1111	Click
01/01/2013 16:17:34	911	Inbound	555-333-2222	Click
01/01/2013 21:09:12	911	Inbound	555-333-4444	Click
01/01/2013 23:12:45	Admin	Inbound	555-333-4444	Click

Exhibit 83. Individual Call Detail Report Example



Individual Call Detail
Generated: mm/dd/yyyy hh:mm:ss

Seizure Date Time: mm/dd/yyyy hh:mm:ss
Call Type: 911
Inbound/Outbound: Inbound
Abandoned: No
Answer seconds: 3
Duration seconds: 123
Position answered: 6
Operator answered: Operator 1
Transferred: No
Transfer records: N/A
ANI: 555-123-5678
Location information: Address 1, City, State, Zip Code, XY Coordinates
Class of Service: WPH2
Carrier: Carrier1

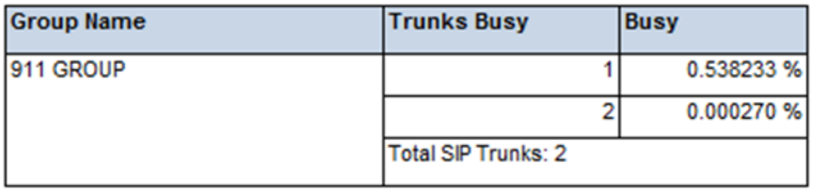
Raw Data:

<xmlexample>

Exhibit 84. Individual Call Detail Report Example

Summary of Call Loads

Summary of Call Loads can be addressed in multiple ways. The first is call volume. Call volume can be addressed through the Event Summary report as detailed above. In addition, call loads can be reported on in terms of the PSAP’s ability handle a certain number of incoming or active calls at any given time. The ‘Utilization Report’ provides data on the percentage of time in a given data range that multiple SIP trunks are in simultaneous use. This provides information as to whether the PSAP continually has ability to handle incoming calls (particularly in a high volume situation), or if the PSAP encounters times where no incoming calls will be accepted.



Group Name	Trunks Busy	Busy
911 GROUP	1	0.538233 %
	2	0.000270 %
	Total SIP Trunks: 2	

Exhibit 85. Utilization Report Example

5.3.1 EVENT REPORTS

Event reporting shall record the timing of transit for each payload for purposes of diagnostics.

All event reports shall, at a minimum, include the functional element being reported and the system time of such event.

The system shall provide, at a minimum, the following event reports:

- Time of payload entry through BCF;
- Time for each functional element to perform routing and PSAP assignment;
- Time of answer at PSAP; and
- Time of disconnect at PSAP.
- A cumulative total elapsed time for payloads to traverse the system.

Times shall be stored as Coordinated Universal Time (UTC) and converted to local time based on the User Profile.

Times shall be stored in 24 hour format including thousands of a second.

2015-07-31 20:51:20.537 UTC – for example

The system shall provide a Time Server on the ESInet using the Network Time Protocol (NTP). PSAPs will be offered use of this Time Server to synchronize the clocks on their 9-1-1 CPE, workstations, etc.

Respondents shall describe their proposed solution for event reporting functionality.

TCS Response: Comply.

ECaTS will provide an i3 compliant logging service interface which aggregates logs from the Network (ex: an ESInet) and the Call Handing System to support end to end transaction logging and retrieval. ECaTS is optimized as a “transaction logger”, capturing meta data for all payloads to provide end to end reports. ECaTS is compliant to the i3 specification for recording of the transaction meta data. All times captured and computed use the NG-911 international UTC standard and ECaTS will synchronize with the network clock used by all NG Functional Elements to ensure synchronized time.

ECaTS supports an i3 compliant web services interface in addition to the standard web interface for retrieval of reporting and data. All significant steps in processing a call are logged by the Network devices/services and call handling systems and submitted to the ECaTS logger. Each log contains a transaction ID to support log aggregation for end to end reporting. The ECaTS logger web services conforms to NENA 8-003 v1 Detailed Functional and Interface Specification for the NENA i3 Solution, Stage 3 Version 1.

ECaTS supports two options for State and PSAP users to access and retrieve i3 transactions and events. The primary method is via the web interface which allows PSAPs to review and retrieve MIS and i3 Log Replication through the current NG SOAP interfaces.

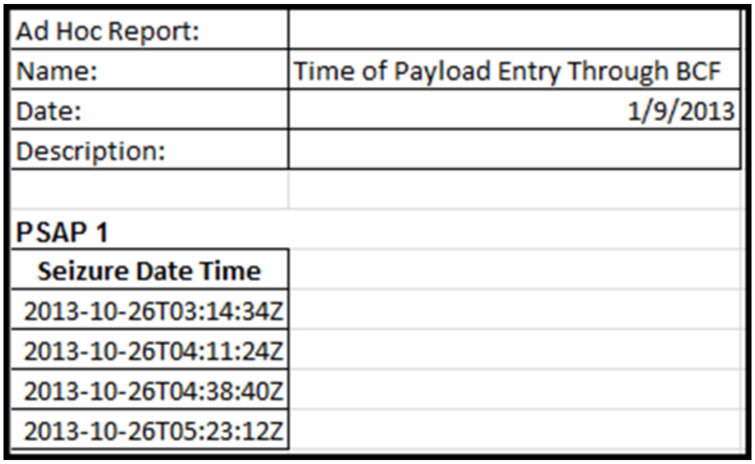
Access to the log replication web services are an add-on as all reporting features are provided through the ECaTS MIS portal. Should the log replication services be licensed, the following web services are implemented as defined by the NG-911 V1/V2 specifications.

- RetreiveLogEvent
- ListEventsByCallId
- ListEventsByIncidentId
- ListCallsByIncidentId
- ListIncidentsByDateRange
- ListIncidentsByLocation
- ListIncidentsByDateAndLocation
- ListCallsByDateRange
- ListAgenciesByCallId

As described above, the ECaTS platform provides general reporting against the collected network data. Additional customized reporting can be created depending on the needs of the Alabama 9-1-1 Board, but included are the following reports:

Time of Payload Entry Through BCF

Time of Payload Entry through BCF report is shown in Exhibit 86. Users can search by a specific time, include or filter by additional desired information, or receive all BCF entry times for a desired time/date range.

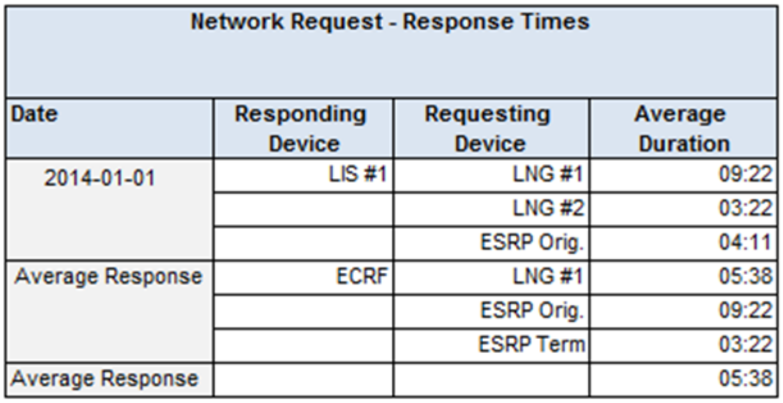


Ad Hoc Report:	
Name:	Time of Payload Entry Through BCF
Date:	1/9/2013
Description:	
PSAP 1	
Seizure Date Time	
2013-10-26T03:14:34Z	
2013-10-26T04:11:24Z	
2013-10-26T04:38:40Z	
2013-10-26T05:23:12Z	

Exhibit 86. Time of Payload Entry Through BCF Report

Time for Each Functional Element To Perform Routing and PSAP Assignment

End to end Routing Report provides information regarding routing performance and PSAP assignment as shown below. This data is also available for ad hoc reporting. Users can search by a specific event, include or filter by desired information, or receive all ECRF routing assignment times for a desired time/date.



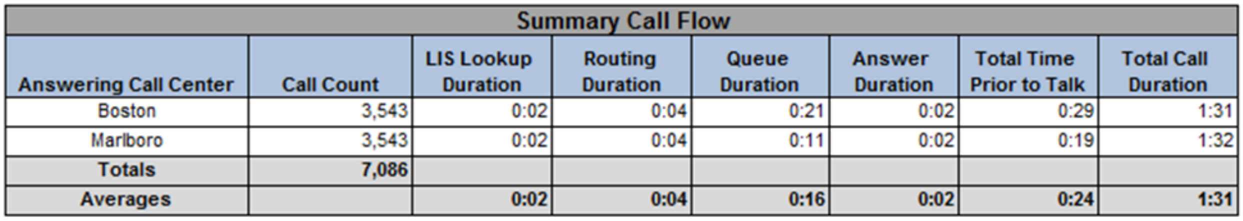
Network Request - Response Times

Date	Responding Device	Requesting Device	Average Duration
2014-01-01	LIS #1	LNG #1	09:22
		LNG #2	03:22
		ESRP Orig.	04:11
Average Response	ECRF	LNG #1	05:38
		ESRP Orig.	09:22
		ESRP Term	03:22
Average Response			05:38

Exhibit 87. End-to-End Routing Report

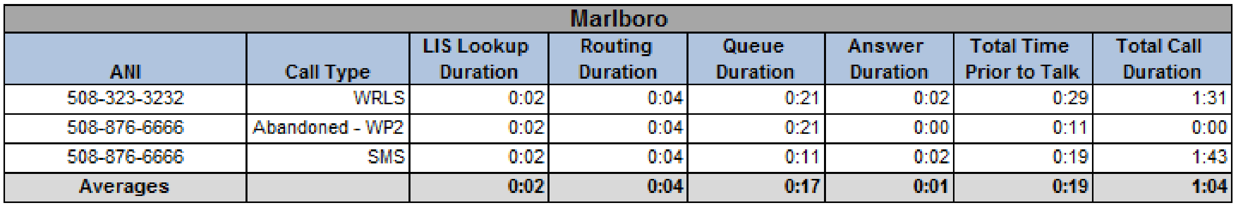
Time of Answer at PSAP

Answer time is calculated from seizure to event answer. This is a field included on the Average Duration report, and is also used to create the PSAP Answer Time report using data supplied by the Call Handling system. In addition, time of answer at PSAP is a value available for reporting in the ad-hoc system.



Summary Call Flow

Answering Call Center	Call Count	LIS Lookup Duration	Routing Duration	Queue Duration	Answer Duration	Total Time Prior to Talk	Total Call Duration
Boston	3,543	0:02	0:04	0:21	0:02	0:29	1:31
Marlboro	3,543	0:02	0:04	0:11	0:02	0:19	1:32
Totals	**7,086**						
Averages		**0:02**	**0:04**	**0:16**	**0:02**	**0:24**	**1:31**



Marlboro							
ANI	Call Type	LIS Lookup Duration	Routing Duration	Queue Duration	Answer Duration	Total Time Prior to Talk	Total Call Duration
508-323-3232	WRLS	0:02	0:04	0:21	0:02	0:29	1:31
508-876-6666	Abandoned - WP2	0:02	0:04	0:21	0:00	0:11	0:00
508-876-6666	SMS	0:02	0:04	0:11	0:02	0:19	1:43
Averages		**0:02**	**0:04**	**0:17**	**0:01**	**0:19**	**1:04**

Exhibit 88. Answer Time Report Example

Time of Disconnect at PSAP

The Disconnect time, or total call duration, can be found in the above report. In addition, PSAP specific reports also include this information in numerous other reports and via ad hoc reporting.

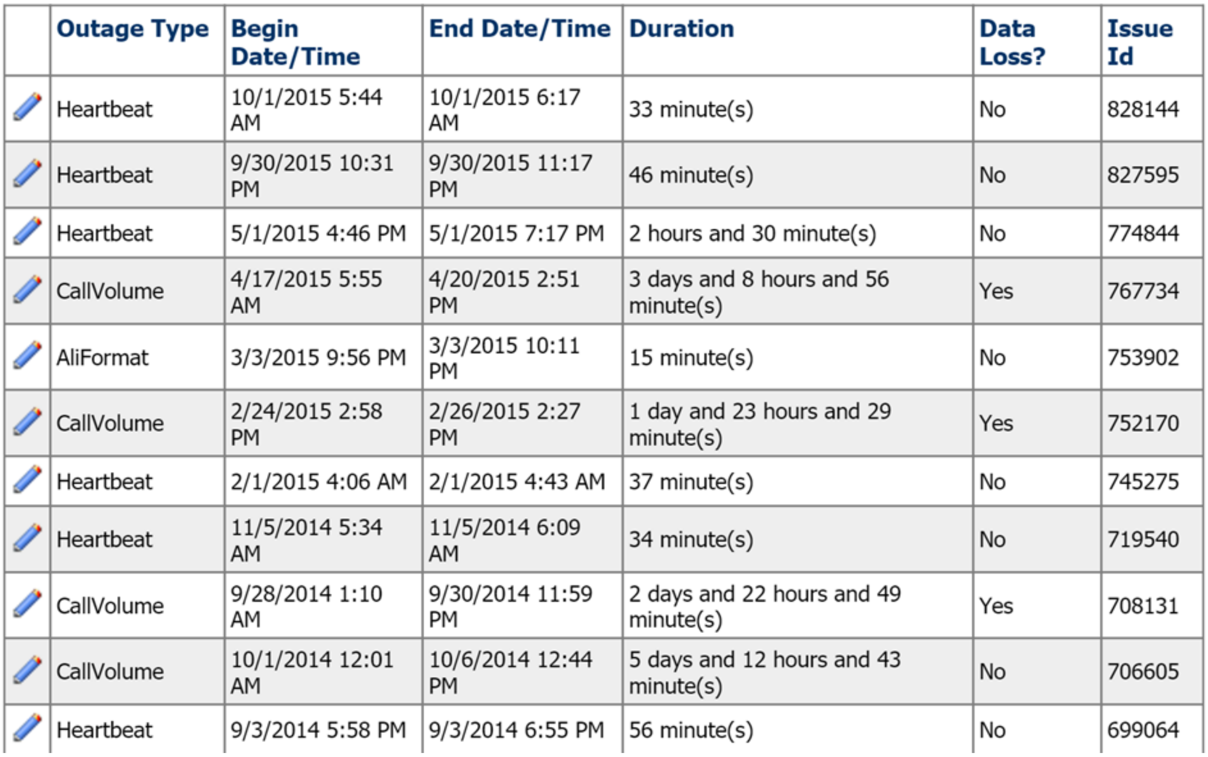
5.3.2 MAINTENANCE / CONFIGURATION REPORTS

- Lists events by date / time range
- Provides drill down to specific events

TCS Response: Comply.

ECaTS provides all detailed maintenance and configuration updates based on system health reporting of issues causing data gathering challenges. ECaTS provides a summary screen of all issues effecting a specific PSAP or a data collector and the ability to drill down into the details of each issue and follow the resolution path and overall results of the maintenance/configuration issue.

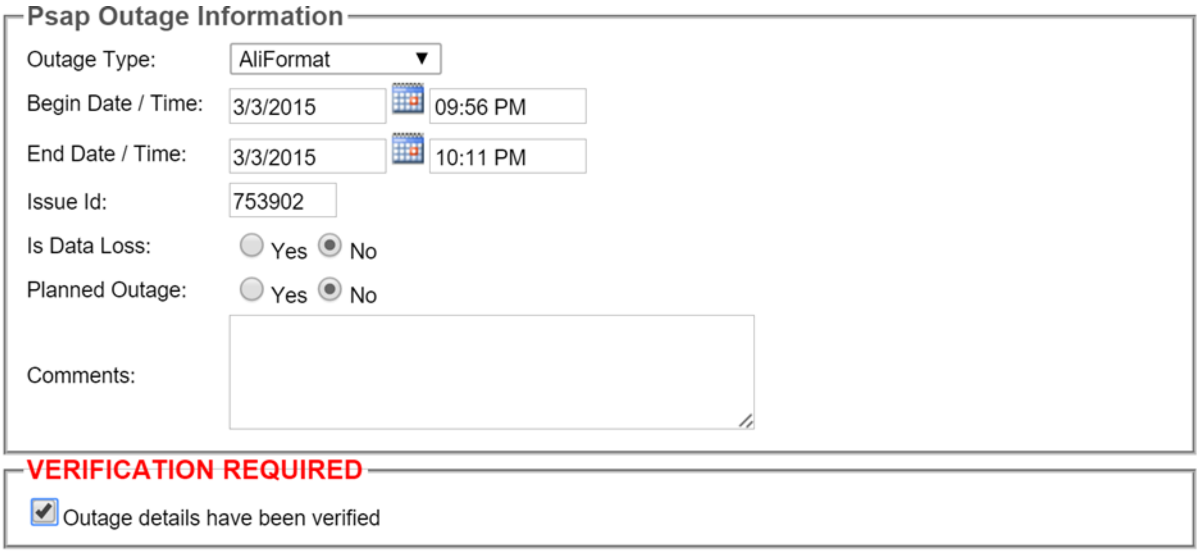
Exhibit 89 is a sample of the maintenance/configuration events list with date/time ranges.



	Outage Type	Begin Date/Time	End Date/Time	Duration	Data Loss?	Issue Id
✎	Heartbeat	10/1/2015 5:44 AM	10/1/2015 6:17 AM	33 minute(s)	No	828144
✎	Heartbeat	9/30/2015 10:31 PM	9/30/2015 11:17 PM	46 minute(s)	No	827595
✎	Heartbeat	5/1/2015 4:46 PM	5/1/2015 7:17 PM	2 hours and 30 minute(s)	No	774844
✎	CallVolume	4/17/2015 5:55 AM	4/20/2015 2:51 PM	3 days and 8 hours and 56 minute(s)	Yes	767734
✎	AliFormat	3/3/2015 9:56 PM	3/3/2015 10:11 PM	15 minute(s)	No	753902
✎	CallVolume	2/24/2015 2:58 PM	2/26/2015 2:27 PM	1 day and 23 hours and 29 minute(s)	Yes	752170
✎	Heartbeat	2/1/2015 4:06 AM	2/1/2015 4:43 AM	37 minute(s)	No	745275
✎	Heartbeat	11/5/2014 5:34 AM	11/5/2014 6:09 AM	34 minute(s)	No	719540
✎	CallVolume	9/28/2014 1:10 AM	9/30/2014 11:59 PM	2 days and 22 hours and 49 minute(s)	Yes	708131
✎	CallVolume	10/1/2014 12:01 AM	10/6/2014 12:44 PM	5 days and 12 hours and 43 minute(s)	No	706605
✎	Heartbeat	9/3/2014 5:58 PM	9/3/2014 6:55 PM	56 minute(s)	No	699064

Exhibit 89. Maintenance/Configuration Events with Date/Time Ranges

For each maintenance/configuration event that is present on the output, clicking the "pencil" icon provides a drill down into a particular issue, Exhibit 90 is a sample of the AliFormat issue details.



Psap Outage Information

Outage Type: AliFormat ▼

Begin Date / Time: 3/3/2015 09:56 PM

End Date / Time: 3/3/2015 10:11 PM

Issue Id: 753902

Is Data Loss: ○ Yes ● No

Planned Outage: ○ Yes ● No

Comments:

VERIFICATION REQUIRED

☑ Outage details have been verified

Exhibit 90. PSAP Outage Notification Showing ALI Format Issue Details

SECTION 6 SERVICE/SUPPORT REQUIREMENTS

6.1 CUSTOMER SUPPORT SERVICES

The ongoing operation of the ANGEN system will require customer support services be provided as a component of any proposed solutions.

Respondents must agree to meet the current Service Level Agreements (SLA) being used in the ANGEN network operation and negotiate “in good faith” new SLA’s that meet the expectations of the functionality described in this RFP and the Board.

Customer support services will be required at various levels including the Board, PSAPs, and other system service providers as necessary or designated by the Board.

Anticipated customer support services would include:

- Event management
- Incident management
- Diagnostics and reporting
- Problem resolution/trouble handling
- Network fault monitoring
- Request fulfillment
- Access management
- Remote diagnostics
- Environmental requirements
- Capacity management
- Change management
- Configuration management
- Transition management

Respondents shall provide a description of their proposed customer service support services.

TCS Response: Comply.

TCS NOC is the first point of contact to provide Customer Support. Our NOC can be contacted 24x7 via our toll-free telephone number at 1.800.959.3749 or by email noc@telecomsys.com. We will work with Alabama to identify the list of Alabama-authorized personnel who require this level of access to the TCS NOC.

The TCS NOC manages our trouble ticket system. Our NOC tools are designed and implemented in a georedundant manner. The NOC is backed by a “dark” NOC in Phoenix, Arizona, complete with failover network management system (NMS) and ticketing systems.

Should the Seattle facility become inoperable, staff will relocate to the Phoenix data center until the Seattle location becomes operable. From Phoenix, they will continue to monitor and troubleshoot the E9-1-1 and networks so emergency services operations occur uninterrupted.

Our NOC monitors our NG9-1-1 solutions, identifying and troubleshooting issues, issuing internal and external notification of incidents, and providing incident management and problem resolution. We will generate a trouble ticket and assign a severity level when service impairment is discovered by or reported to TCS. We track every call event, including call origination, call completion, call control messages, data translations, and ALI database data delivery. We provide monitoring, call handling, troubleshooting, and repair of incidents within our span of control.

TCS maintains an Incident Management Plan (IMP) that details internal policies and procedures for managing service incidents related to our products. The IMP describes the set of actions to be taken by the NOC during a service incident. Our IMP is designed to facilitate the fastest resolution possible such as:

Detection: NOC analysts become aware of and log the incident.

Identification: NOC analysts investigate and assess the incident and determine the severity level. The initial troubleshooting steps are logged in the trouble ticket at this point.

Escalation: NOC analysts escalate the incident to other support tiers and/or to management as warranted by the severity level.

Notification: NOC analysts notify internal and external stakeholders about the incident as required by the severity level and the IMP policies for the affected service. (The IMP policies for each service are described in the IMP module for that service.) Follow-up notification occurs regularly thereafter.

Troubleshooting and Analysis: NOC analysts document the steps being taken to resolve the incident, facilitate communication among relevant parties, and distribute updates.

Resolution: The incident is resolved and the system is restored to full integrity. NOC analysts verify resolution, send final notification of the resolution to all stakeholders, and change the status of the trouble ticket.

RCA: The technical owner and the NOC owner of the high severity trouble tickets complete the RCA on these trouble tickets.

Closure: If necessary, the NOC lead reviews the RCA and sends it to the relevant parties. A NOC analyst or the NOC lead closes the trouble ticket.

At all times during service impairment, the TCS NOC follows established procedures to resolve the impairment. Our responsibilities include creating and updating the trouble ticket, managing escalation, and keeping all stakeholders informed of progress. We notify customers by email.

Our NOC escalates incidents that are beyond its capabilities to appropriate support staff. If requested by the customer, we also can escalate the incident to TCS management. Even after escalation, the primary responsibility for driving an incident to resolution lies with the NOC.

We monitor hardware, network components, and applications to ensure incidents are identified, addressed, and resolved in a timely manner.

Our system monitoring is performed in near real-time using Hewlett-Packard’s OpenView and Network Node Manager products. All events related to security trigger log entries and/or traps. Our monitoring tools alarm when events suggest an attempt at a security breach, such as multiple failed attempts to login.

We will ensure network element configuration data is backed up regularly and will establish recovery processes in the event of catastrophic failure. We will manage the configuration data to restrict unauthorized access. Management of configuration data is performed through a network configuration management tool such as DeviceExpert.

Our change management process follows industry standard. Any routine maintenance tasks are completed through our Implementation and Back-Out Plan (IBOP). For all system change events, we use IBOP documentation, which is similar to the industry-recognized method of procedure (MOP). Before implementing a change, TCS team coordinates a final technical review and a final management review of the proposed IBOP.

In most instances network and change management activities will be conducted without any required involvement from the Agency. The Agency may be asked to provide assistance in certain circumstances.

6.2 HELP DESK

Respondents shall provide help desk services as a component of their proposed solution.

The help desk(s) shall operate on a 24x7x365 basis and be adequately staffed by resources that are trained and qualified in help desk and customer support services.

The help desk shall serve as a single point of contact for all matters, including without limitation, the system, all components of the system, and any additional system service providers delivering services or components for the network ecosystem.

The help desk must not use an automated attendant or other automated means to answer calls for service or trouble.

The help desk must be accessible via various methods including voice, text, email, and other means as deemed appropriate by the Board.

The help desk shall have the ability to communicate directly and immediately with maintenance and support services for the proposed system and all components of the proposed system, including without limitation, network troubles.

Respondents shall describe and explain their proposed help desk services.

TCS Response: Comply.

Upon the identification of a service-affecting issue, the customer should contact the TCS Network Operations Center (NOC) to open a trouble ticket. The TCS NOC can be reached by calling 1-800-959-3749 or by sending an email to noc@telecomsys.com.

Upon receiving customer notification of an issue, the NOC will work the issue, escalating appropriately to ensure timely resolution. The NOC reviews all tickets on the day they are received. The NOC sends out impairment notifications, impairment updates, and notifications of resolution to all impacted parties for SIL 1 (critical) or SIL 2 (major) outages.

6.3 TROUBLE HANDLING AND TICKETING REQUIREMENTS

Trouble handling and trouble ticket tracking services will be required.

To ensure that all trouble tickets are resolved in a timely manner, respondents shall propose an escalation guideline document that describes the escalation procedure.

The current ANGEN system utilizes the following procedures. Respondents may use this as a guide for their proposed system.

1. **Critical – Network outage**

- 1st Level Support – Within 15 minutes
- Continuous problem resolution/workaround effort
- 2nd Level Support – within 2 Hours
- 3rd Level Support – within 4 Hours or upon Customer request.

2. **Major – Service effecting**

- 1st Level Support – Within 15 minutes
- 2nd Level Support – Within 4 Hours
- 3rd Level Support – Within 24 Hours or upon Customer request.

3. **Minor – Non-service effecting**

- 1st Level Support – Within 30 minutes
- 2nd Level Support – Within 1 business day
- 3rd Level Support - Within 1 week or upon Customer request.

4. **Planned Maintenance/Informational – Software update, configuration.**

- 1st Level Support – Within 2 Hours
- 2nd Level Support – Within 5 Business days
- 3rd Level Support – Only upon Customer or Management request.

Following any critical event or major outage, the Board must receive a root cause analysis within five (5) business days.

Respondents shall provide a description of their root cause analysis process and what documentation is provided upon the conclusion of the analysis.

Respondents shall describe their trouble management and ticketing process.

Respondents shall provide details of how trouble tickets are generated, documented, resolved and reported.

TCS Response: Comply.

The NOC is responsible for monitoring network connections, ALI database connections, and NG9-1-1 production operations. For NG9-1-1 production operations, TCS monitors all interfaces, connections, services, and processes as well as issues that encompass loading, distribution, messaging, and performance.

Incidents are reported to the customer based upon Service Impact Level (SIL). TCS defines four SILs as shown in Exhibit 91. The SIL determines the responsibilities of the TCS NOC when responding to an impairment of service within the systems or service parameters TCS is obligated to provide under its Service Level Agreement (SLA).

For each SIL, TCS has a target resolution time, shown in Exhibit 91.

During any SIL 1 or SIL 2 incident, the TCS NOC keeps the customer regularly informed as to the status of the situation, providing assistance until the incident is resolved or until the situation has been downgraded from its critical status. Assisted by TCS, the customer helps determine when the situation is no longer an emergency.

The categorization of an event as SIL 1, SIL 2, SIL 3, or SIL 4 is made reasonably by TCS based upon the definitions shown in Exhibit 91; all SIL 1, SIL 2, events are communicated to the customer as early as possible, based upon the best information available at the time. TCS ensures its response is made by an appropriately qualified technician, and within the time frames shown in Exhibit 91.

TCS notifies the customer NOC by email, using the most current contact information on file for that customer. All communications sent to the customer by TCS include the TCS trouble ticket number. Final RCA reports for SIL 1 or SIL 2 events are typically sent within 10 business days.

Exhibit 91. SIL Table

Severity Level	Description	Notification	Target Resolution
1 – Critical	▪ 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 (for example, no delivery of either ANI or ALI)	▪ Initial response to PSAP occurs, as soon as possible but no longer than one hour after incident identification ▪ Subsequent updates occur hourly via email	▪ A configuration change or a procedure for customer to bypass or work-around the anomaly in order to continue operations- not to exceed 4 hours ▪ If bypass or work-around is provided, TCS shall continue good faith resolution efforts. ▪ Remediations will be shared with customer
2 – High	▪ 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 ▪ (For example, no delivery of either ANI or ALI, for a particular class of service).	▪ Initial response to PSAP occurs, via email, as soon as possible but no longer than two hours after incident identification. ▪ Subsequent updates occur at least every 12 hours via email	▪ A configuration change or a procedure for customer to bypass or work-around the anomaly in order to continue operations- not to exceed 24 hours ▪ If bypass or work-around is provided, TCS shall continue good faith resolution efforts. ▪ Remediations will be shared with customer

Severity Level	Description	Notification	Target Resolution
3 – Medium	▪ Non-critical system failure that causes performance degradation or system components to malfunction. ▪ Reported problems disabling specific non-essential functions; error condition is not critical to continuing operations and/or work-around has been determined for the error condition	▪ N/A	▪ Workaround or Temporary fix within less than 10 business days ▪ Code Correction in a next regular update or maintenance release ▪ If bypass or work-around 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	▪ 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.	▪ N/A	▪ Code correction in a 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 work- around solution to customer.

6.4 TRAINING

Respondents shall work cooperatively with the Board to ensure training programs are conducted for the proposed solution. Respondents shall provide training for the network operations and support functions including:

At the PSAP:

- Network Status Reports
- Help Desk
- Text to 9-1-1 operation
- Trouble Ticketing

At the AL9-1-1 Board:

- Network Status Reports
- Help Desk

- Trouble Ticketing
- Root Cause Analysis and review

Respondents shall provide a proposed training plan and sample documentation and materials for the training detailed above.

TCS Response: Comply.

We will work with Alabama to determine the curriculum content for training.

Our certified trainers have extensive experience in implementing training programs for all TCS solutions, using proven techniques to provide hands-on training in a workshop environment that simulates how the TCS solutions operate in the real world. TCS' trainers provide a combination of classroom presentations and hands-on interaction, focusing on the functional and technical aspects of the software.

These software trainers work with the manager of training and technical writing to identify any customized training the customer may require. The manager of training and technical writing generates a plan that identifies prerequisites, individual session objectives, and the duration of the training sessions. TCS also provides a training syllabus that outlines the agenda and topics covered during each training session.

Training Plan

The TCS certified trainer will conduct the training session. At a high-level, the agenda that will be presented is the following:

- Managed Network Services and ALI Database Management
- What Is Changing?
- TCS Service Delivery Overview
  - TCS Roles and Responsibilities
- Managed Network Overview
  - Benefits of Managed Network Service
- TCS NOC Introduction
  - Example of TCS NOC Presentation and Training
  - TCS Tier 1 Support
  - Notifications
  - Monitoring
  - PSAP Monitoring
  - Reporting a 911 Trouble to TCS NOC
  - TCS Issues a Managed Service SOP
- TCS ALI Database Management System

- PSAP Benefits of the State of Alabama ALI Database/TCS Database Management System
- What Comprises an ALI
- Master Street Address Guide – MSAG (NENA 02-010, v. 2.1)
- What is SOI?
- How does a Customer Telephone Number Record get validated?
- ESN and ELT (Police, Fire and EMS data)
- Time of Call ALI Format Spill
- How Will You Access Your ALI Data?
- You Can Search For ALI Records In Your Region
- You Can Download Full ALI Data
- MSAG Records and Downloads
- TCS MSAG Change Request Workflow
- ECD (PSAP) Comment Field
- ECD/PSAP Comment Field
- Live Demonstration of TCS ALI Features for ECDs/PSAPs
- How To Contact TCS For ALI Issues

- Deployment Overview – ALI
  - Project Plan
  - Deployment Overview
- NG9-1-1 ESInet Overview (Optional)
  - NG9-1-1 ESInet Solution Overview
  - ESInet Design Considerations / Implementation Approach
  - ESInet PSAP Components
- NG9-1-1 Call Flow
  - Design Considerations / Implementation Approach
  - PSAP Site Visits

Full documentation and training syllabi will be provided after negotiating a specific training agenda with state of Alabama personnel.

6.5 MONITORING OF APPLICATIONS AND EQUIPMENT

Proposed solutions will require proactive monitoring of all system components for operation, performance and fault conditions.

The proposed solution shall ensure that all alarms including environmental status alarms are received and monitored in a Network Operations Center (NOC).

Respondents shall describe the tools, methods and procedures that will be used for monitoring.

Respondents shall include a matrix of components that will be proactively monitored, managed and administered.

TCS Response: Comply.

TCS provides carriers with continuous availability of its systems on a 24x7 basis. Using highly available facilities to maintain the standards necessary to accommodate the emergency services field, TCS follows detailed provisioning and operations procedures to maintain network integrity. TCS designs, builds and provisions its systems to be reliable, highly available, auto-aware, and fault resilient. TCS Operations builds and monitors its systems in a production environment.

Exhibit 92. TCS Network Operations Center

Monitoring is provided by the TCS NOC. The TCS NOC is ISO 27001, and ISO 9001-certified. It provides continuous, subscription-based service designed to deliver real-time protection to the enterprise. The TCS NOC will:

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

The services available with TCS NOC monitoring include:

- Availability monitoring
- Event handling
- Event monitoring
- Event correlation
- Event escalation
- Co-location of critical services
- Disaster recovery
- Post-event analysis
- Incident response

- Policy-based incident handling, based on Service Level Agreement (SLA)
- Packet analysis
- Respond/restore/remediate
- Feed and receive incident alerts
- Monthly incident reporting based on SLA requirements

6.6 NETWORK OPERATIONS CENTER

The proposed solution requires the services of a Network Operations Center (NOC).

The NOC must operate on a 24x7x365 basis for the duration of the contract.

In addition, the NOC shall include the capability to perform remote maintenance and restoration of alarms as necessary.

The NOC shall be the single point that performs continuous monitoring, maintenance and network support services.

The NOC shall interface with the help desk.

The NOC shall be staffed with appropriate technical resources to aid trouble shooting, diagnosis and recovery from issues.

The NOC shall perform monitoring of the entire network, all connections and functional components used to provide ANGEN services.

The NOC shall be equipped with a Network Management System (NMS) that monitors the performance of the network and infrastructure.

- The NMS shall continuously monitor the performance and availability of all devices
- The NMS shall monitor network performance, including throughput, latency, jitter, packet loss, and other parameters deemed necessary by the Board
- The NMS shall monitor the network for network intrusion attempts security breaches and be capable of issuing security alerts when an event is recognized
- The NMS shall create alarms based on thresholds and parameters and distribute alarm notifications appropriately
- The NMS shall monitor the environment at all data centers or points of presence where critical network components are housed to ensure functionality
- The NMS shall monitor ancillary network components such as power utilization and backup power systems

Respondents shall describe the capabilities of their proposed NOC, including the proposed NMS system and provide details regarding its operation and the ability of the NOC to interface with other providers and systems.

TCS Response: Comply.

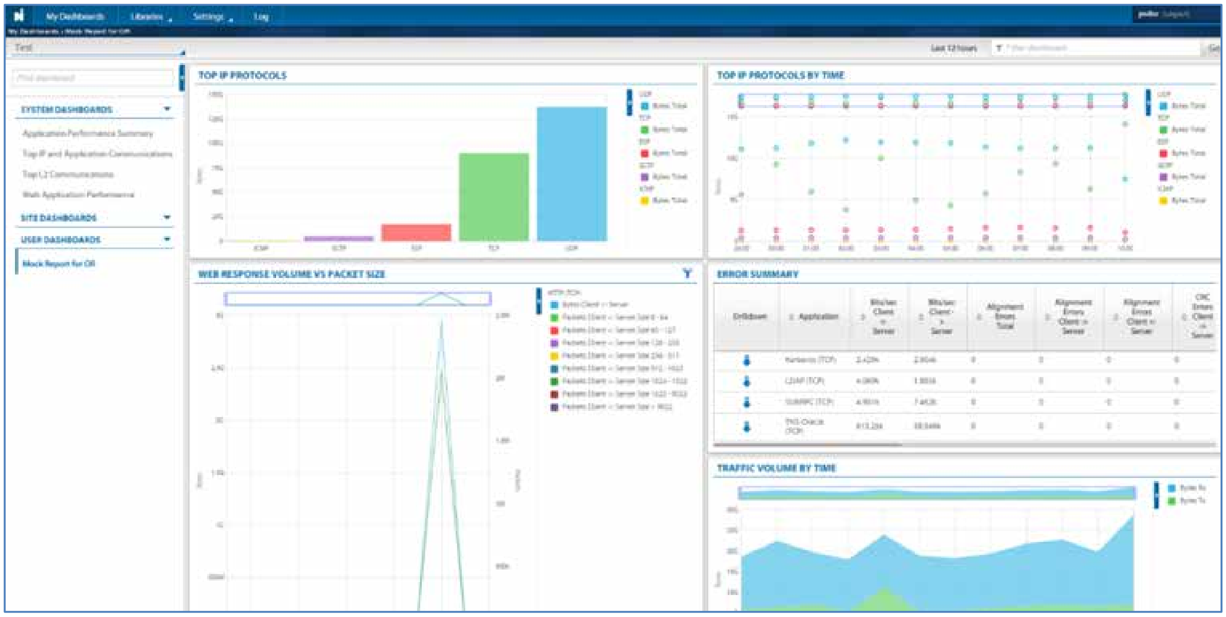
TCS maintains a 24x7, state-of-the-art, carrier-grade NOC. The NOC provides NG9-1-1 services to wireless carriers, upholds the high standards necessary for emergency services, and follows detailed provisioning and operations procedures to maintain network integrity at 99.999 percent.

The NOC is responsible for identification, troubleshooting, internal and external notification of incidents, incident management, and problem resolution. Every call event is tracked, including call origination, call completion, call control messages, data translations, and ALI database data delivery. A comprehensive disaster recovery plan is in place that details procedures, processes, and training. In the event of a catastrophic failure in the Seattle NOC, the Phoenix NOC provides backup and resumes operation of the system as the primary NOC.

Managed Network Services (MNS)

TCS can provide a number of monitoring capabilities through its managed services products. TCS' managed services are tailored specifically to the unique needs of next generation IP-based network deployments. These managed services include network monitoring and anti-virus protection management.

We use the powerful Observer performance management platform from Network Instruments for both real-time and historical operational performance metrics in our managed network services (MNS) offering. Observer creates aggregated views of network health with real-time application health and edge-to-core retrospective network analysis using the Gigastor product. This network analysis package offers extensive insight and management of our network solution, and we will use it to deliver historical reports as part of our performance reporting. Historical reports can be generated on an hourly, daily, weekly, monthly, and annual interval, when required. A sample MNS report is shown in Exhibit 93.



Drilldown	Application	Bits/sec Client -> Server	Bits/sec Client <- Server	Alignment Errors Total	Alignment Errors Client -> Server	Alignment Errors Client <- Server	CRC Errors Client -> Server
	Kerberos (TCP)	2.42M	2.95M	0	0	0	0
	LDAP (TCP)	4.08M	1.88M	0	0	0	0
	SUNRPC (TCP)	4.90M	7.46M	0	0	0	0
	TNS Oracle (TCP)	815.2K	88.54M	0	0	0	0

Exhibit 93. Sample MNS Report

Monitoring service is designed to deliver continued real-time protection to the enterprise. It will:

- Detect quickly
- Notify stakeholders
- Respond appropriately
- Restore critical services
- Provide complete RCA for SIL 1 and SIL 2 events (high impact to service)

TCS is the only noncarrier TL 9000-certified organization that supports E9-1-1 services. Our solutions and services are backed by:

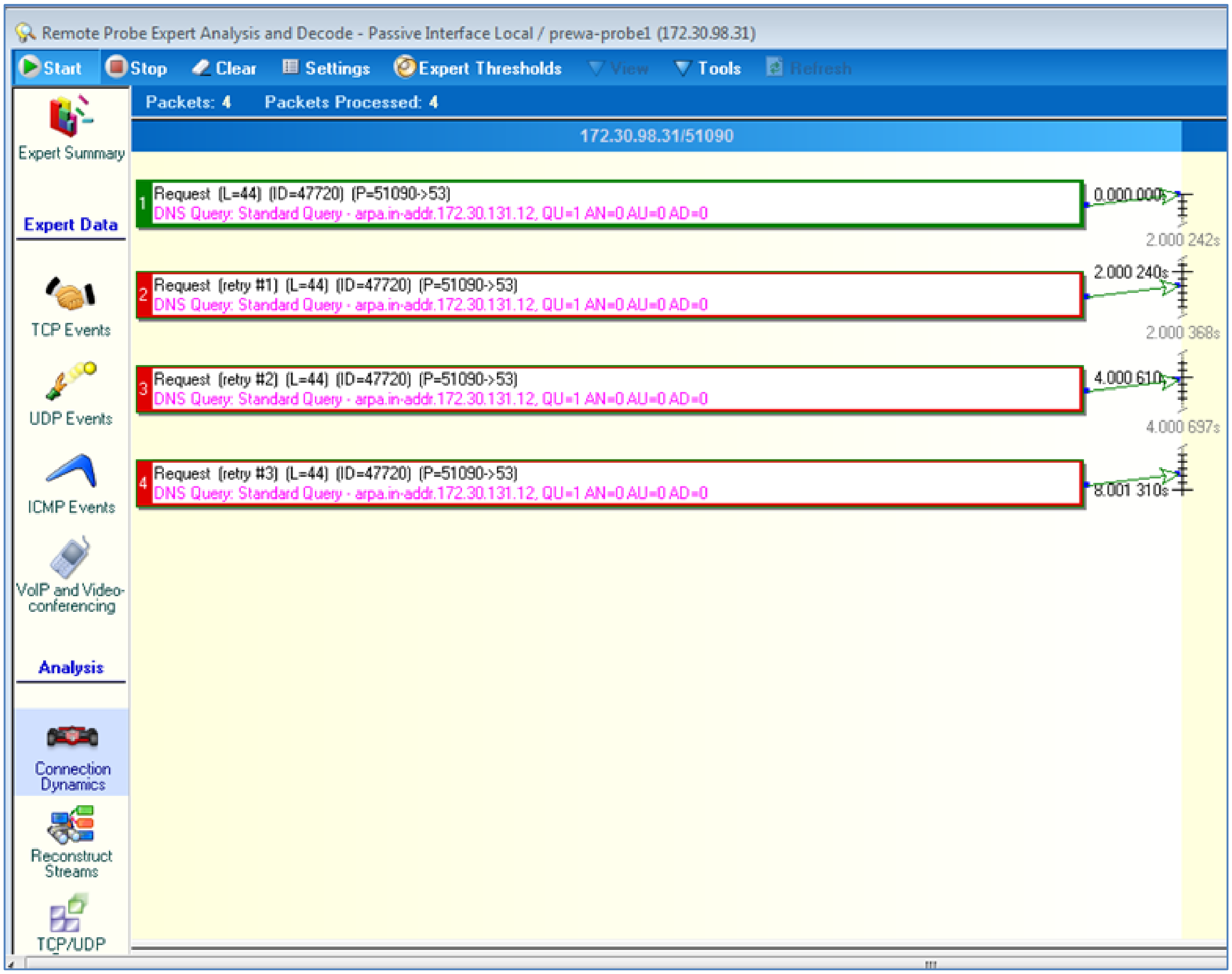
- ISO 27001, ISO 9001, and TL 9000 certification

- 24x7 monitoring and operations support
- Georedundant advanced network monitoring and reporting tools (HP OpenView, Remedy, etc.) optimized by full-suite vendor support and TCS-trained engineers
- High retention of monitoring staff (seven years) and engineers (nine years)

The services available with TCS NOC monitoring include:

- Availability monitoring
- Event handling
- Event monitoring
- Event correlation
- Event escalation
- Co-location of critical services
- Disaster recovery
- Post-event analysis
- Incident response
- Policy-based incident handling, based on SLA
- Packet analysis
- Respond/restore/remediate
- Feed and receive incident alerts
- Deliverables
- Monthly health check
- Monthly incident reporting based on SLA requirements
- TL 9000 continuous process improvement

Our monitoring includes comprehensive analysis of network events, furthering our ability to troubleshoot and maintain the network. Exhibit 94 shows an event analysis screenshot.



Packets: 4 Packets Processed: 4

172.30.98.31/51090

1 Request (L=44) (ID=47720) (P=51090->53)
DNS Query: Standard Query - arpa.in-addr.172.30.131.12, QU=1 AN=0 AU=0 AD=0
0.000 000s
2.000 242s

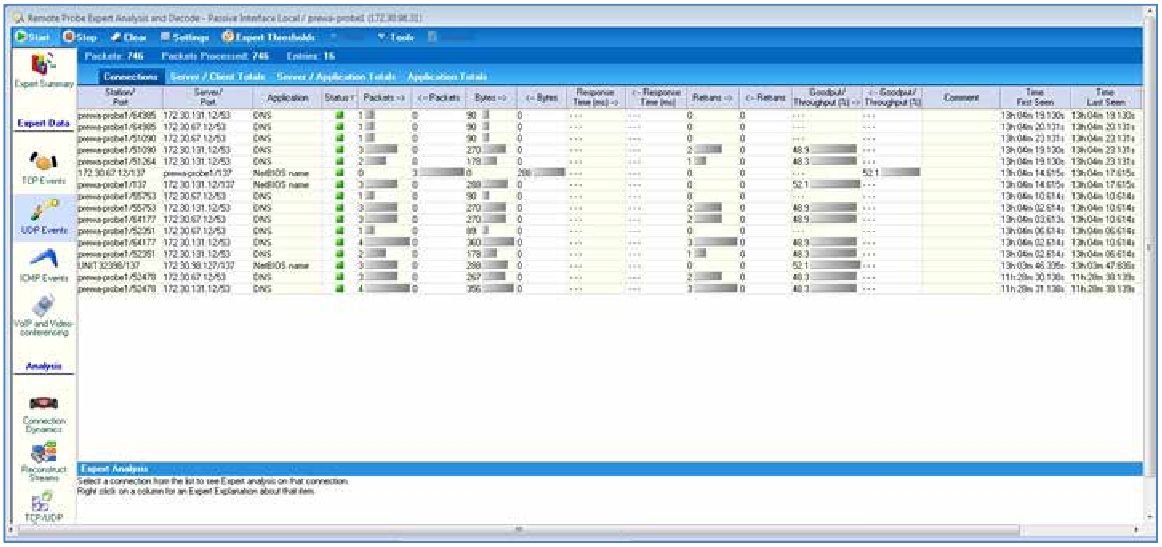
2 Request (retry #1) (L=44) (ID=47720) (P=51090->53)
DNS Query: Standard Query - arpa.in-addr.172.30.131.12, QU=1 AN=0 AU=0 AD=0
2.000 240s
2.000 368s

3 Request (retry #2) (L=44) (ID=47720) (P=51090->53)
DNS Query: Standard Query - arpa.in-addr.172.30.131.12, QU=1 AN=0 AU=0 AD=0
4.000 610s
4.000 697s

4 Request (retry #3) (L=44) (ID=47720) (P=51090->53)
DNS Query: Standard Query - arpa.in-addr.172.30.131.12, QU=1 AN=0 AU=0 AD=0
8.001 310s

Exhibit 94. Event Analysis Screenshot

Exhibit 95 shows the granular detail the decoding interface provides.



Packets: 746 Packets Processed: 746 Entries: 16

Station/ Port	Server/ Port	Application	Status	Packets ->	<- Packets	Bytes ->	<- Bytes	Response Time (ms) ->	<- Response Time (ms)	Retrans ->	<- Retrans	Goodput/ Throughput (%) ->	<- Goodput/ Throughput (%)	Comment	Time First Seen	Time Last Seen
prewa-probe1/54985	172.30.131.12/53	DNS	🟩	1	0	90	0	---	---	0	0	---	---		13h:04m 19.130s	13h:04m 19.130s
prewa-probe1/54985	172.30.67.12/53	DNS	🟩	1	0	90	0	---	---	0	0	---	---		13h:04m 20.131s	13h:04m 20.131s
prewa-probe1/51090	172.30.67.12/53	DNS	🟩	1	0	90	0	---	---	0	0	---	---		13h:04m 23.131s	13h:04m 23.131s
prewa-probe1/51090	172.30.131.12/53	DNS	🟩	3	0	270	0	---	---	2	0	48.9	---		13h:04m 19.130s	13h:04m 23.131s
prewa-probe1/51264	172.30.131.12/53	DNS	🟩	2	0	178	0	---	---	1	0	48.3	---		13h:04m 19.130s	13h:04m 23.131s
172.30.67.12/137	prewa-probe1/137	NetBIOS name	🟩	0	3	0	288	---	---	0	0	---	52.1		13h:04m 14.615s	13h:04m 17.615s
prewa-probe1/137	172.30.131.12/137	NetBIOS name	🟩	3	0	288	0	---	---	0	0	52.1	---		13h:04m 14.615s	13h:04m 17.615s
prewa-probe1/55753	172.30.67.12/53	DNS	🟩	1	0	90	0	---	---	0	0	---	---		13h:04m 10.614s	13h:04m 10.614s
prewa-probe1/55753	172.30.131.12/53	DNS	🟩	3	0	270	0	---	---	2	0	48.9	---		13h:04m 02.614s	13h:04m 10.614s
prewa-probe1/64177	172.30.67.12/53	DNS	🟩	3	0	270	0	---	---	2	0	48.9	---		13h:04m 03.613s	13h:04m 10.614s
prewa-probe1/52351	172.30.67.12/53	DNS	🟩	1	0	89	0	---	---	0	0	---	---		13h:04m 06.614s	13h:04m 06.614s
prewa-probe1/64177	172.30.131.12/53	DNS	🟩	4	0	360	0	---	---	3	0	48.9	---		13h:04m 02.614s	13h:04m 10.614s
prewa-probe1/52351	172.30.131.12/53	DNS	🟩	2	0	178	0	---	---	1	0	48.3	---		13h:04m 02.614s	13h:04m 06.614s
UNIT32398/137	172.30.98.127/137	NetBIOS name	🟩	3	0	288	0	---	---	0	0	52.1	---		13h:03m 46.335s	13h:03m 47.836s
prewa-probe1/52478	172.30.67.12/53	DNS	🟩	3	0	267	0	---	---	2	0	40.3	---		11h:28m 30.138s	11h:28m 38.139s
prewa-probe1/52478	172.30.131.12/53	DNS	🟩	4	0	356	0	---	---	3	0	40.3	---		11h:28m 31.138s	11h:28m 38.139s

Expert Analysis

Select a connection from the list to see Expert analysis on that connection.
Right click on a column for an Expert Explanation about that item.

Exhibit 95. Network Performance – Interface Data Example

6.7 ALARM CATEGORIES

The proposed solution shall provide categories of alarms by event types depending on the criticality of the event (i.e. critical, major, etc.).

The proposed system shall allow for the dynamic configuration of notification thresholds as well as the ability to define new alarm categories as necessary.

The system shall provide for the automatic notification of the NOC when alarm conditions are detected.

Different notification and escalation procedures may apply depending on alarm category.

Respondents shall describe how alarms are received and specify what types of alarms are available for viewing/receiving and how and when they are generated.

TCS Response: Comply.

The NOC is responsible for monitoring network connections, ALI database connections, and NG9-1-1 production operations. For NG9-1-1 production operations, TCS monitors all interfaces, connections, services, and processes as well as issues that encompass loading, distribution, messaging, and performance.

Alarm events generate Simple Network Management Protocol (SNMP) traps that are gathered and analyzed by the TCS NOC staff.

Incidents are reported to the customer per Service Impact Level (SIL). TCS defines four SILs. The SIL determines the responsibilities of the TCS NOC when responding to an impairment of service within the systems or the service parameters that TCS is obligated to provide under the Service Level Agreement (SLA). For each SIL, TCS has a target resolution time.

During any SIL 1 or SIL 2 incident, the TCS NOC keeps the customer regularly informed as to the status of the situation and provides assistance until the incident is resolved, or until the situation has been downgraded from a critical status. Assisted by TCS, the customer helps to determine when the situation is no longer an emergency.

The categorization of an event as SIL 1, SIL 2, SIL 3, or SIL 4 is reasonably made by TCS based upon the definitions in Exhibit 91; all SIL 1, SIL 2, events are communicated to the customer as early as possible, based upon the best information available at the time. TCS ensures the response is made by an appropriately qualified technician within the time frame shown in Exhibit 91 in Section 6.3.

TCS notifies the customer NOC by 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.

6.8 SCHEDULED MAINTENANCE

The proposed system requires a scheduled maintenance process.

The process must include a methodology for coordinating and scheduling preventative maintenance activities and how those events are executed.

During scheduled maintenance activities the network and system shall not experience a degradation or disruption.

However, individual components may be taken down for maintenance if an alternate route or redundant system is used to minimize the effect.

Respondents shall describe how their schedule maintenance process will work.

TCS Response: Comply.

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 is typically written over a several-week period and includes multiple meetings where engineers discuss the best design, review impacted services, 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.

SECTION 7 ELECTRICAL, WIRING, AND CABLE REQUIREMENTS

7.1 ELECTRICAL

Successful respondents shall provide and maintain all electrical, wiring, and cable services necessary for their proposed system.

Successful respondents shall provide electrical services as follows:

- Supply and install where needed and otherwise maintain existing complete electrical power distribution system for all equipment supplied.
- Provide adequate surge protection, grounding and lightning suppression devices to protect equipment from unnecessary interruption.
- Provide and maintain a minimum level of thirty (30) minute uninterruptible power supply for all equipment supplied.

Respondents shall provide all necessary cabinets, tables, stands, or other required mounting facilities for their proposed system.

Respondents shall adhere to FCC and all local codes and ordinances in all matters pertaining to the work.

TCS Response: Comply.

TCS agrees to comply with all applicable national, state and local codes and regulations. The proposed solution uses Commercial Off-the-Shelf (COTS) equipment that complies with all appropriate Federal Communications Commission (FCC), Underwriters Laboratories (UL)/ Canadian Standards Association (CSA), Conformité Europééne (CE), and National Emergency Number Association (NENA) standards—as they apply to such elements as electrical safety, electromagnetic interference—for computer and telecommunications equipment.

7.2 ELECTRICAL INTERFERENCE

All devices proposed for the system shall be provided with any and all necessary connecting cords and cables conforming to National Electrical Manufacturers Association (NEMA) codes.

The system shall not cause interference to the existing radio, security, or closed circuit television communications systems, installed communications console equipment, or other data processing equipment present in the operational environment, and, in addition, shall comply with all applicable FCC standards as applied to data processing equipment.

TCS Response: Comply.

TCS agrees to comply with all applicable national, state and local codes and regulations. The proposed solution uses Commercial Off-the-Shelf (COTS) equipment that complies with all appropriate Federal Communications Commission (FCC), Underwriters Laboratories (UL)/ Canadian Standards Association (CSA), Conformité Europééne (CE), and National Emergency Number Association (NENA) standards—as they apply to such elements as electrical safety, electromagnetic interference—for computer and telecommunications equipment.

7.3 WIRING AND CABLING

All interface connections and visible cables shall use standard EIA connectors secured by wall plates where exposed.

All cables shall be clearly marked and/or numbered in a manner that reflects a unique identifier of the cable at both ends.

Any cables used shall be plenum rated where required by local building or fire codes.

Respondents shall ensure that all equipment is connected to emergency AC power and is configured to be supported by a UPS.

Cabling, communications outlets, power wiring, system grounding, conduit facilities, and equipment rooms shall be installed in accordance with national standards and applicable local codes.

Minimum standards used in the installations shall include, but are not limited to, the following:

- ANSI/TIA/EIA-568 - Commercial Building Telecommunications Wiring Standard
- ANSI/TIA/EIA-569 - Commercial Building Standard for Telecommunications Pathways and Spaces
- ANSI/TIA/EIA-606 - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings
- ANSI/TIA/EIA-607 - Commercial Building Grounding and Bonding Requirements for Telecommunications
- Building Industry Consulting Service International, Telecommunications Distribution Methods Manual
- National Electrical Code (NFPA-70)
- FCC Rules and Regulations, Parts 68 and 15

TCS Response: Comply.

All TCS equipment is plugged into appropriate power distribution units (PDUs) and Uninterruptible Power Supply (UPS) at each site.

Power requirements for each data center requires a direct connection to common building ground for grounding and bonding of the equipment rack, in addition to NEMA 5-20R power connections within three feet of the base of the TCS equipment racks.

The engineering design for the central equipment at each data center and at each PSAP includes the appropriate grounding according to accepted telecommunications installation standards.

Our preventive network maintenance program is tied to our proactive monitoring managed service. This service is intended to detect potential issues and correct them before they impact service.

With regard to the PSAP remote locations, we perform routine maintenance twice a year. Such routine maintenance is scheduled with each PSAP and typically includes the following:

- Verify with site staff there are no issues with the equipment.
- Verify all system equipment power supplies are powered and show no alarm states.
- Verify all equipment connectivity cabling is securely connected.
- Verify the rack environment is clean and clear of all obstructions.

7.4 GROUNDING

The proposed system shall provide surge and lightning protection for all connections to AC power.

All hardware and peripheral devices shall be mechanically and electrically grounded to prevent both user hazard and loss of data or hardware integrity due to external electrical impulse.

Respondents shall ground all equipment in compliance with manufacturer recommendations and applicable standards.

Respondents shall furnish and install the required grounding and bonding conductors where necessary and complete the connections to the grounding system at all sites.

TCS Response: Comply.

The proposed solution assumes a ground bar is available in the equipment rack, capable of supporting additional external grounding cables.

Team members responsible for installing the equipment that comprises this proposed solution have undergone significant training and are well versed in the standards and practices that align with the process of providing adequate system grounding. The team agrees to comply with all applicable national, state and local codes and regulations.

7.5 TRANSIENT VOLTAGE SURGE SUPPRESSION

In addition to primary protection, secondary Transient Voltage Surge Suppression (TVSS) shall be installed with the proposed system where appropriate.

Respondents shall implement TVSS that meets the following criteria

- TVSS devices shall be installed on all equipped ports that are connected to; or may be connected to wireline or wireless facilities.
- The secondary TVSS devices shall be listed with a maximum clamping voltage of 250 volts (.5kV) or less and operate in less than 10 nanoseconds.
- All TVSS devices shall meet UL497A requirements and shall have an operational indicator to alert maintenance personnel that the device has been utilized, failed or that the circuit is unprotected.
- The secondary TVSS shall not degrade the audio signaling.

TCS Response: Comply.

The solution also includes full transient voltage surge suppression (TVSS) protection, including lightning protection.

SECTION 8 PROJECT MANAGEMENT AND PLANNING REQUIREMENTS

8.1 IMPLEMENTATION PROJECT PLAN

Respondents shall provide a project management plan that identifies the methodology for implementing their proposed solution. The implementation project management plan shall be consistent with Project Management Institute (PMI) best practices.

At a minimum the implementation project plan must include:

- Schedule.
- Change management plan.
- Configuration management plan.
- Communications plan.
- Quality Assurance and Quality Control plan.
- Risk management plan.
- Status report and dashboard tools.
- Proposed Site by site implementation/work plan

The Project Plan will be referred to on a regular basis during the implementation phase of the project to ensure that implementation is completed in a timely fashion.

Any changes to the schedule and work plan must be communicated to the Board through the proposed Change Management process.

The project plan shall clearly define the milestones and clearly identify when the transition from implementation into service management occurs.

TCS Response: Comply.

The professionals who staff the TCS Project Management Office (PMO) have extensive training and experience with managing complex, multi-tiered projects. They are fluent in managing Emergency Services Internet Protocol Network (ESInet), Internet Protocol (IP) based call handling, Automatic Location Identification (ALI) Database Management System (DBMS), and Geographic Information System (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.

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.

A project manager will be assigned to oversee the seamless transition, cutover, and restoration of the proposed solution. This project manager will have had extensive training and experience in managing complex, multi-tiered projects, thereby ensuring that these solutions will meet Alabama's needs, even beyond project implementation and cutover. The entire project management team has been assembled to offer all the guidance necessary for a success transition to the proposed Next Generation 9-1-1 (NG9-1-1) solution.

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 system settings and configurations
- A system acceptance test plan
- Standard technical and maintenance information
- As-built diagrams and drawings of the system's layout and design.

The overarching plan involves a number of stages, described below, 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 Alabama to perform and document system data collection activities, with special attention given to such unique site conditions as space constraints, wiring requirements, and telco demarcs.

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.

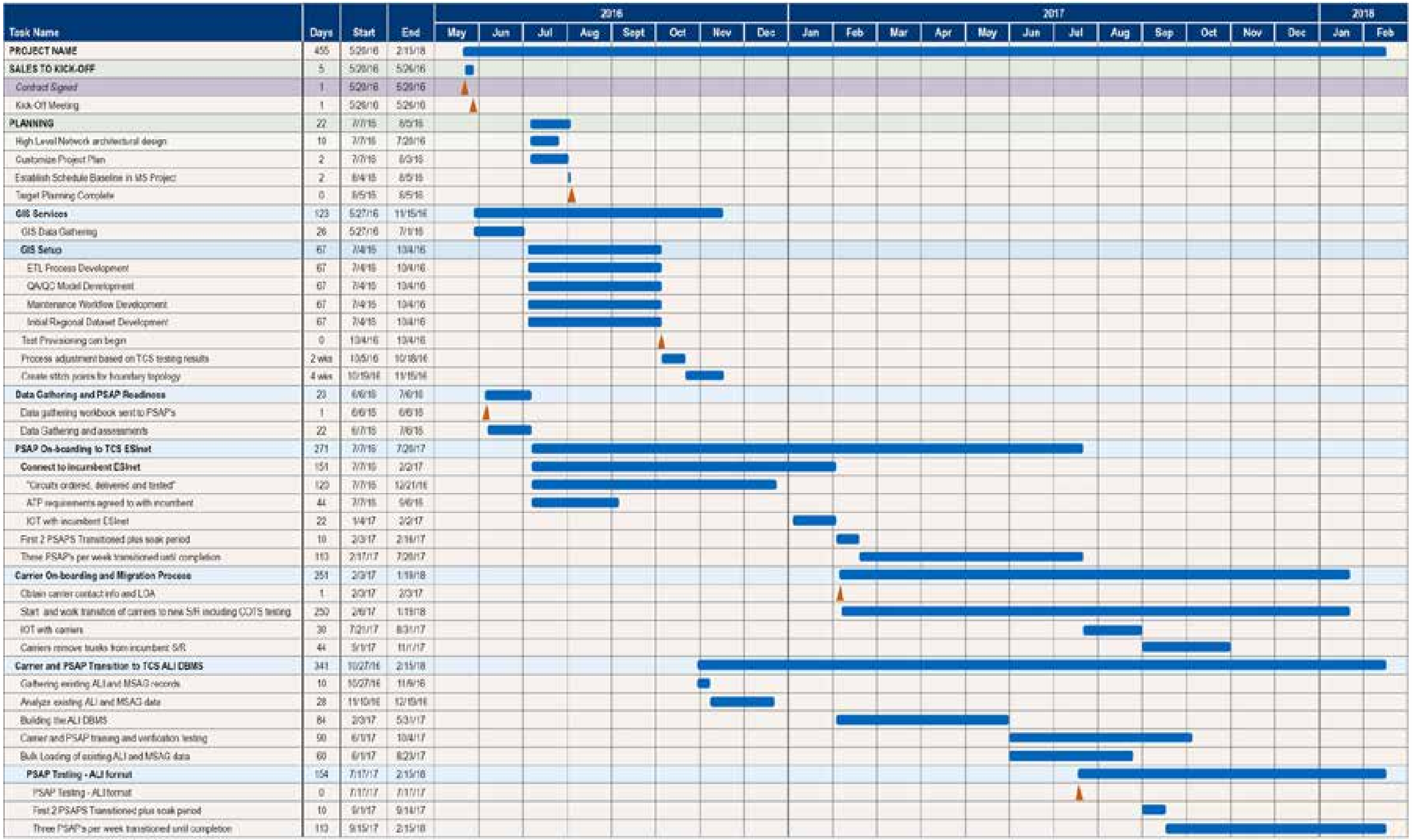
Installation – The installation stage, which is minimal as it pertains to PSAPs, includes such elements as site preparation, running cable, populating the PSAP-provided racks with the proper hardware, and checking for proper power levels and network connectivity. All personnel charged with performing 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 in Montgomery and Huntsville.

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. Initial failover and redundancy testing occurs offline, with routing to the new system pre-cut so as to minimize any risk to live traffic.

Exhibit 96 shows a sample ESInet implementation project schedule. Details for an Alabama implementation schedule can be built once specific details are known.



Task Name	Days	Start	End
PROJECT NAME	455	5/26/16	2/15/18
SALES TO KICK-OFF	5	5/20/16	5/26/16
Contract Signed	1	5/20/16	5/20/16
Kick-Off Meeting	1	5/26/16	5/26/16
PLANNING	22	7/7/16	8/5/16
High Level Network architectural design	10	7/7/16	7/20/16
Customize Project Plan	2	7/7/16	8/3/16
Establish Schedule Baseline in MS Project	2	8/4/16	8/5/16
Target Planning Complete	0	8/5/16	8/5/16
GIS Services	123	5/27/16	11/15/16
GIS Data Gathering	26	5/27/16	7/1/16
GIS Setup	67	7/4/16	10/4/16
ETL Process Development	67	7/4/16	10/4/16
QA/QC Model Development	67	7/4/16	10/4/16
Maintenance Workflow Development	67	7/4/16	10/4/16
Initial Regional Dataset Development	67	7/4/16	10/4/16
Test Provisioning can begin	0	10/4/16	10/4/16
Process adjustment based on TCS testing results	2 wks	10/5/16	10/18/16
Create stitch points for boundary topology	4 wks	10/19/16	11/15/16
Data Gathering and PSAP Readiness	23	6/6/16	7/6/16
Data gathering workbook sent to PSAP's	1	6/6/16	6/6/16
Data Gathering and assessments	22	6/7/16	7/6/16
PSAP On-boarding to TCS ESInet	271	7/7/16	7/28/17
Connect to incumbent ESInet	151	7/7/16	2/2/17
"Circuits ordered, delivered and tested"	120	7/7/16	12/21/16
ATP requirements agreed to with incumbent	44	7/7/16	9/6/16
IOT with incumbent ESInet	22	1/4/17	2/2/17
First 2 PSAPS Transitioned plus soak period	10	2/3/17	2/16/17
Three PSAP's per week transitioned until completion	113	2/17/17	7/28/17
Carrier On-boarding and Migration Process	251	2/3/17	1/19/18
Obtain carrier contact info and LOA	1	2/3/17	2/3/17
Start and work transition of carriers to new S/R including COTS testing	250	2/6/17	1/19/18
IOT with carriers	30	7/21/17	8/31/17
Carriers remove trunks from incumbent S/R	44	9/1/17	11/1/17
Carrier and PSAP Transition to TCS ALI DBMS	341	10/27/16	2/15/18
Gathering existing ALI and MSAG records	10	10/27/16	11/9/16
Analyze existing ALI and MSAG data	28	11/10/16	12/19/16
Building the ALI DBMS	84	2/3/17	5/31/17
Carrier and PSAP training and verification testing	90	6/1/17	10/4/17
Bulk Loading of existing ALI and MSAG data	60	6/1/17	8/23/17
PSAP Testing - ALI format	154	7/17/17	2/15/18
PSAP Testing - ALI format	0	7/17/17	7/17/17
First 2 PSAPS Transitioned plus soak period	10	9/1/17	9/14/17
Three PSAP's per week transitioned until completion	113	9/15/17	2/15/18

Exhibit 96. Intrepid9-1-1 ESInet Implementation Schedule

8.2 SYSTEM TEST PLAN

System testing of any new implementations will be required prior to the Board authorizing any cutover to full operational status and the commencement of payment for services.

Respondents must anticipate and plan for all necessary system testing for each service, component, function, application or piece of equipment comprising the proposed solution.

The proposed test plan shall include, but not be limited to testing for:

- i3 functional element testing
- ESInet throughput and capacity testing
- ESInet end to end connectivity testing
- Fault tolerance testing
- ESInet failover and alternate route testing
- ESInet monitoring systems
- Fault notification
- Firewalls, intrusion detection systems, intrusion protection systems

Respondents shall provide an example system test plan that tests each element of their proposed system.

TCS Response: Comply.

TCS will work with the state of Alabama 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.

CLC Test Plan

The test plan is proprietary information, so it is excluded from this proposal. Instead, we offer Exhibit 97 and Exhibit 98, which depict the table of contents of our test plan. TCS has used test plans such as this in previous successful ESInet deployments.

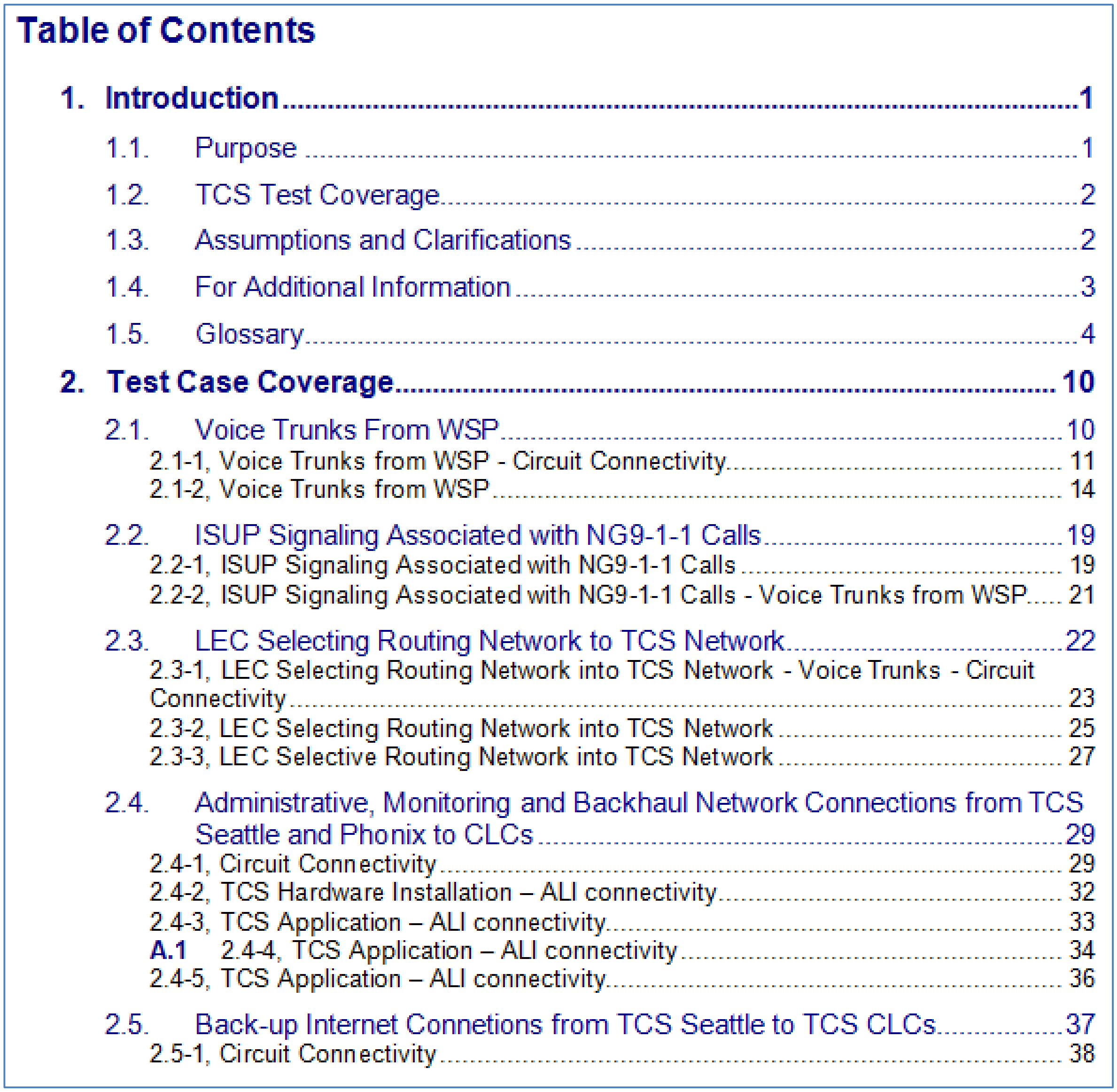
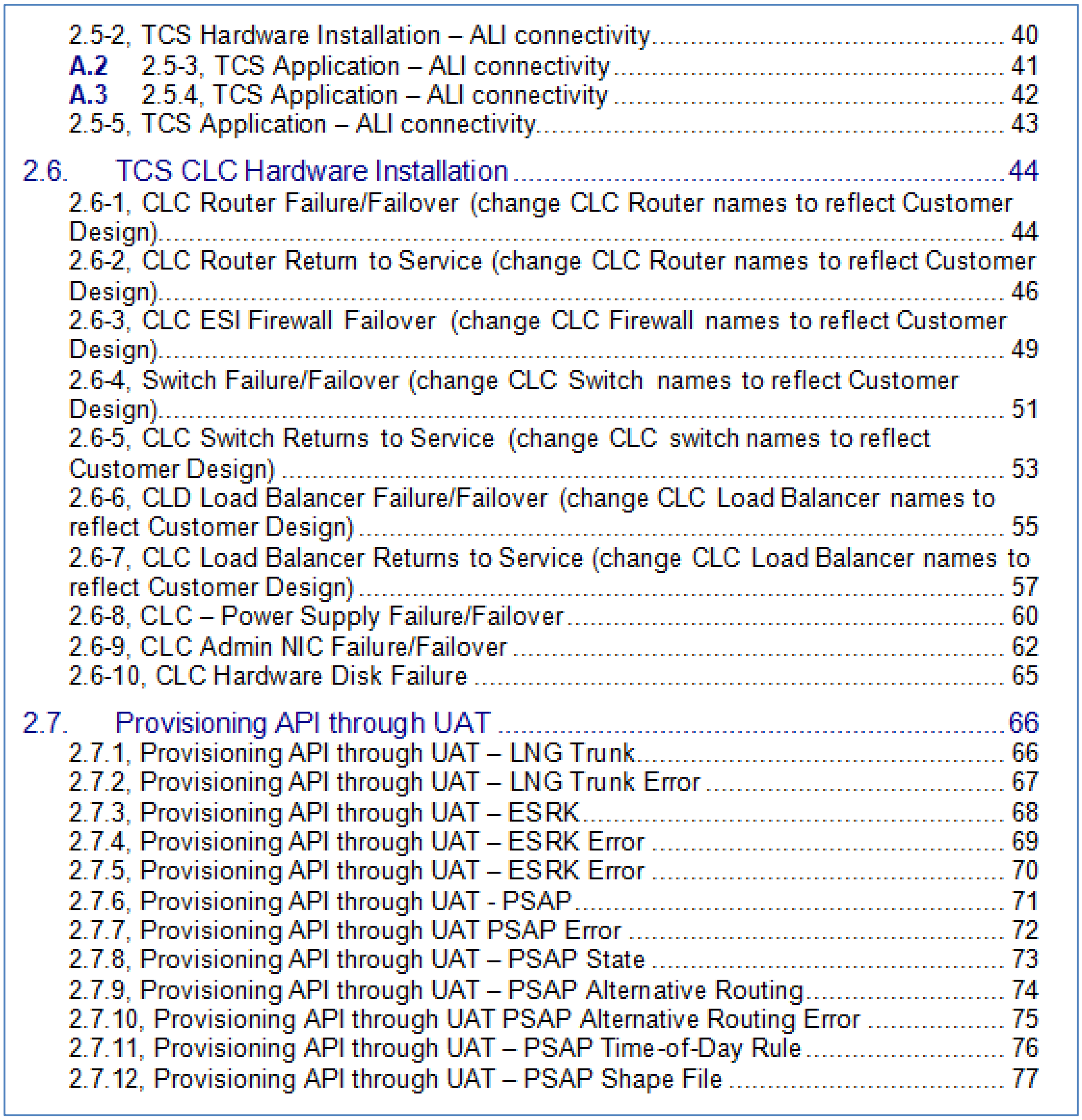


Table of Contents

1. Introduction 1
1.1. Purpose 1
1.2. TCS Test Coverage 2
1.3. Assumptions and Clarifications 2
1.4. For Additional Information 3
1.5. Glossary 4
2. Test Case Coverage 10
2.1. Voice Trunks From WSP 10
2.1-1, Voice Trunks from WSP - Circuit Connectivity 11
2.1-2, Voice Trunks from WSP 14
2.2. ISUP Signaling Associated with NG9-1-1 Calls 19
2.2-1, ISUP Signaling Associated with NG9-1-1 Calls 19
2.2-2, ISUP Signaling Associated with NG9-1-1 Calls - Voice Trunks from WSP 21
2.3. LEC Selecting Routing Network to TCS Network 22
2.3-1, LEC Selecting Routing Network into TCS Network - Voice Trunks - Circuit Connectivity 23
2.3-2, LEC Selecting Routing Network into TCS Network 25
2.3-3, LEC Selective Routing Network into TCS Network 27
2.4. Administrative, Monitoring and Backhaul Network Connections from TCS Seattle and Phonix to CLCs 29
2.4-1, Circuit Connectivity 29
2.4-2, TCS Hardware Installation – ALI connectivity 32
2.4-3, TCS Application – ALI connectivity 33
A.1 2.4-4, TCS Application – ALI connectivity 34
2.4-5, TCS Application – ALI connectivity 36
2.5. Back-up Internet Connetions from TCS Seattle to TCS CLCs 37
2.5-1, Circuit Connectivity 38

Exhibit 97. CLC Test Plan Table of Contents 1 of 2



2.5-2, TCS Hardware Installation – ALI connectivity 40
A.2 2.5-3, TCS Application – ALI connectivity 41
A.3 2.5.4, TCS Application – ALI connectivity 42
2.5-5, TCS Application – ALI connectivity 43

2.6. TCS CLC Hardware Installation 44
2.6-1, CLC Router Failure/Failover (change CLC Router names to reflect Customer Design) 44
2.6-2, CLC Router Return to Service (change CLC Router names to reflect Customer Design) 46
2.6-3, CLC ESI Firewall Failover (change CLC Firewall names to reflect Customer Design) 49
2.6-4, Switch Failure/Failover (change CLC Switch names to reflect Customer Design) 51
2.6-5, CLC Switch Returns to Service (change CLC switch names to reflect Customer Design) 53
2.6-6, CLD Load Balancer Failure/Failover (change CLC Load Balancer names to reflect Customer Design) 55
2.6-7, CLC Load Balancer Returns to Service (change CLC Load Balancer names to reflect Customer Design) 57
2.6-8, CLC – Power Supply Failure/Failover 60
2.6-9, CLC Admin NIC Failure/Failover 62
2.6-10, CLC Hardware Disk Failure 65

2.7. Provisioning API through UAT 66
2.7.1, Provisioning API through UAT – LNG Trunk 66
2.7.2, Provisioning API through UAT – LNG Trunk Error 67
2.7.3, Provisioning API through UAT – ESRK 68
2.7.4, Provisioning API through UAT – ESRK Error 69
2.7.5, Provisioning API through UAT – ESRK Error 70
2.7.6, Provisioning API through UAT - PSAP 71
2.7.7, Provisioning API through UAT PSAP Error 72
2.7.8, Provisioning API through UAT – PSAP State 73
2.7.9, Provisioning API through UAT – PSAP Alternative Routing 74
2.7.10, Provisioning API through UAT PSAP Alternative Routing Error 75
2.7.11, Provisioning API through UAT – PSAP Time-of-Day Rule 76
2.7.12, Provisioning API through UAT – PSAP Shape File 77

Exhibit 98. CLC Test Plan Table of Contents 2 of 2

PSAP Test Plan

The PSAP test plan is proprietary information, so it is excluded from this proposal. Instead, we offer the table of contents for the test plan in Exhibit 99. TCS will use the PSAP test plan to ensure successful PSAP connectivity to the Alabama ESInet.

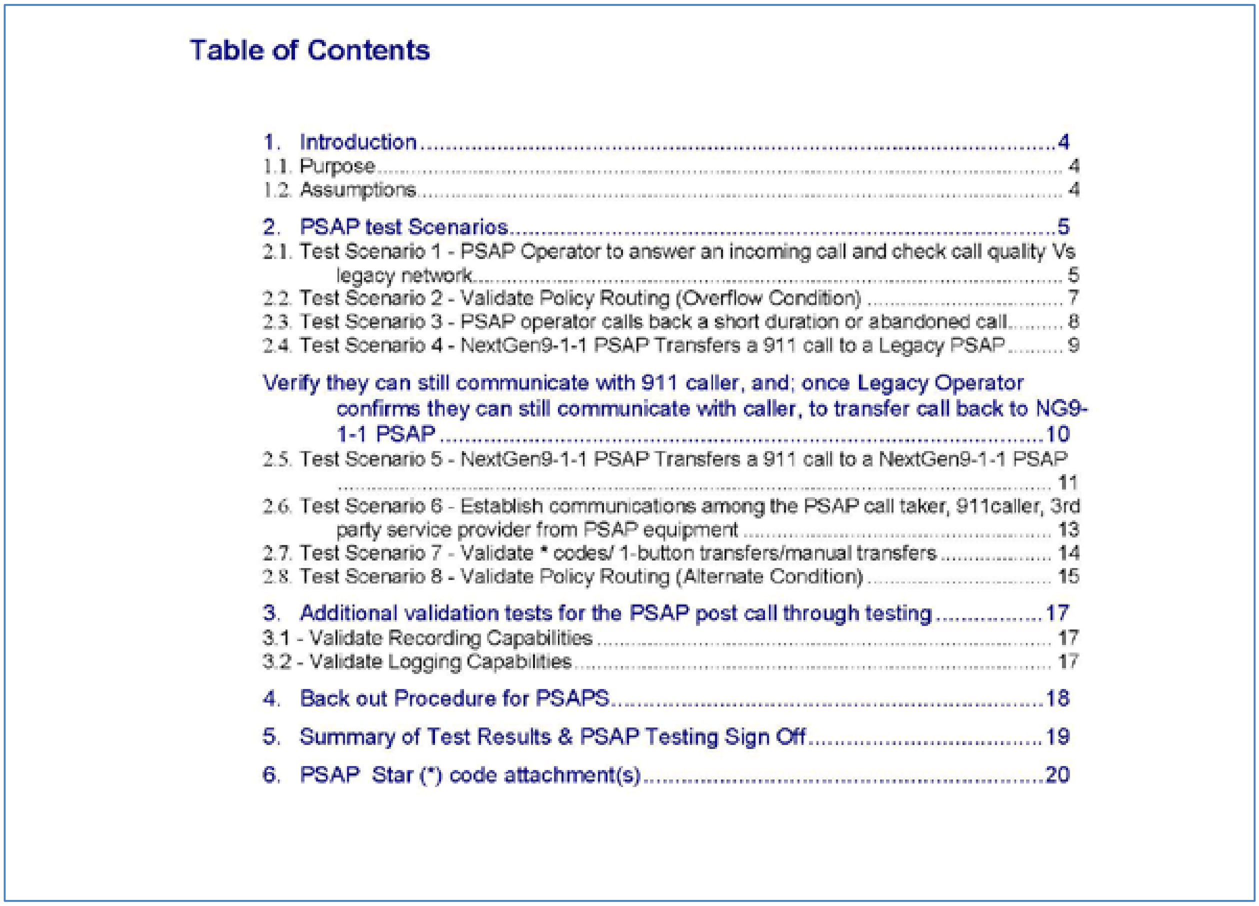


Table of Contents

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 10
2.5. Test Scenario 5 - NextGen9-1-1 PSAP Transfers a 911 call to a NextGen9-1-1 PSAP 11
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

Exhibit 99. PSAP Test Plan Table of Contents

8.3 TRANSITION PLAN

The results of this procurement may require a transition from current ANGEN systems, services and providers to new or different systems, services and providers.

Respondents must anticipate and articulate a plan for the implementation, testing and transition of their proposed systems or services to the point of full operational readiness and cutover to full operation.

This plan may need to anticipate the integration with other systems, services and providers that will comprise the ANGEN system depending on what solutions or services a respondent proposes to provide.

Respondents must provide a proposed transition plan for their systems or services in their response that address the following areas at a minimum:

1. Transition schedule including milestone dates for design, development, testing and implementation phases necessary to achieve full operational readiness and cutover to full operation

2. System testing approach

3. Site cutover approach

4. Contingency or roll back plans should implementation or integration failures occur during the transition or cutover of the proposed systems or services

5. Identification of risks, dependencies or interdependencies that may impact the transition to full operational status and cutover

6. Identification and definition of the ability to support a phased migration and parallel operation with current ANGEN operations

Throughout this anticipated transition period, current ANGEN wireless 9-1-1 call delivery, existing features, functions, capabilities and operations must not be limited or impacted in any fashion by the Respondents.

Respondents are required to work closely with other providers and to cooperate to the fullest extent possible in order to accomplish successful transition to the new ANGEN systems and services created by this RFP.

TCS Response: Comply.

The transition plan is proprietary information, so it is excluded from this proposal. Instead, we offer Exhibit 100 that depicts the table of contents of our transition plan.

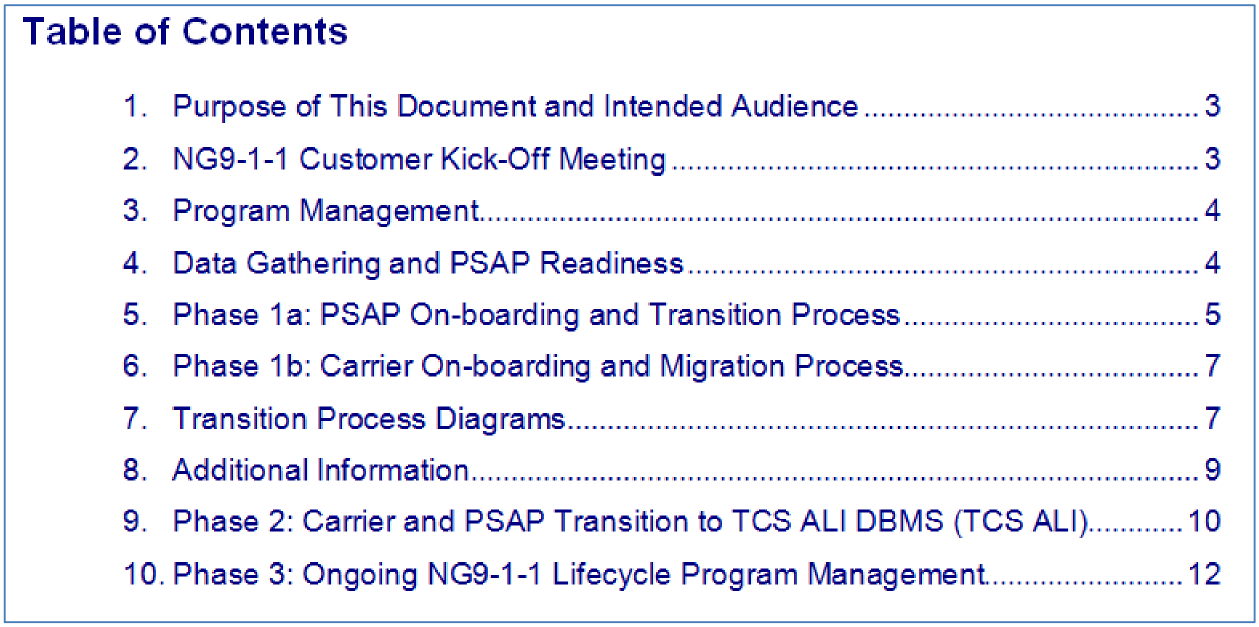


Table of Contents

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. Phase 1a: PSAP On-boarding and Transition Process 5
6. Phase 1b: Carrier On-boarding and Migration Process 7
7. Transition Process Diagrams 7
8. Additional Information 9
9. Phase 2: Carrier and PSAP Transition to TCS ALI DBMS (TCS ALI) 10
10. Phase 3: Ongoing NG9-1-1 Lifecycle Program Management 12

Exhibit 100. Transition Plan Table of Contents

8.4 SERVICE MANAGEMENT PLAN

Oversight of the ESInet and network functions after implementation is required. The preferred best practice is to utilize Information Technology Infrastructure Library (ITIL) as a guideline for how services are designed, implemented, managed, maintained and improved within a lifecycle.

ITIL integrates five stages of service delivery into a comprehensive methodology for managing the lifecycle of services.

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Within these stages, are specific areas relating to Information Technology Service Management.

At a high level, these areas reference how a service maintains availability, capability, capacity, security, manageability, and operability.

Respondents shall describe their approach to service management for the operation of the system. The service management approach shall incorporate components of ITIL or follow industry best practices for IT service management.

Respondents shall provide a narrative of how their proposed service management approach is integrated into their project management activities. Respondents shall discuss their ability to maintain consistent performance and the service levels of the network

TCS Response: Comply.

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

We have demonstrated success with executing large integration projects and global managed network solutions using established, industry-standard program management practices and effective, organized approaches for solution delivery. Our executive management team is committed to the success of this engagement and will assign key personnel to support the Alabama program. A director-level project manager possesses complete authority to successfully execute the program and has full access to whatever critical resources are required for the successful implementation of this program.

2. Cybersecurity Assessment Option

2.1. TCS Security Solutions: Let Us Help Protect the Assets You Can’t Afford to Lose

We believe cybersecurity must be a foundational component of any E9-1-1 network resiliency plan. As with other aspects of E9-1-1 network resiliency, we encourage the use of existing standards, procedures, and specifications. In particular, the NENA Security for NG9-1-1 Standard (NG-SEC) document provides a tenable and vetted approach to cybersecurity in the NG9-1-1 environment and can act as an important planning tool for legacy 9-1-1 networks as they consider transitions to NG9-1-1 platforms. In fact, the NG-SEC standard requirements should be part of any/all RFPs issued for new NG9-1-1 networks.

With this type of forethought to safeguarding NG9-1-1 systems, public safety agencies can ensure that their levels of security and availability are commensurate with their duty to protect and serve their communities.

In order to understand an organization’s security posture, the TCS team of security engineers, technicians, and certified ethical hackers offer vulnerability assessments, penetration tests, and Red Team exercises to evaluate the security effectiveness of an application, an individual machine, or an enterprise.

We submit this proposal to examine the ability of the state of Alabama's system to endure deliberate, malicious attempts (both internal and external) to compromise its network, and subsequently to validate its security posture via the comprehensive security assessment methods outlined below:

- Internal vulnerability assessment
- Web application assessment
- Wireless network security assessment
- External vulnerability assessment
- Written report and executive briefing.

2.2. Comprehensive Security Assessment

We will use our proven and effective security assessment methodology to conduct a comprehensive security assessment on the state of Alabama’s public safety network infrastructure. This infrastructure—whether legacy or NG9-1-1—often contains network connectivity to other infrastructure elements such as record management systems, CAD, call-taker positions (CPE), land mobile radio (LMR), text-to-911, Smart911, and other backend databases such as MSAG, ALI, GIS, and Criminal Justice Information Services (CJIS). Exhibit 101 below shows typical PSAP connectivity.

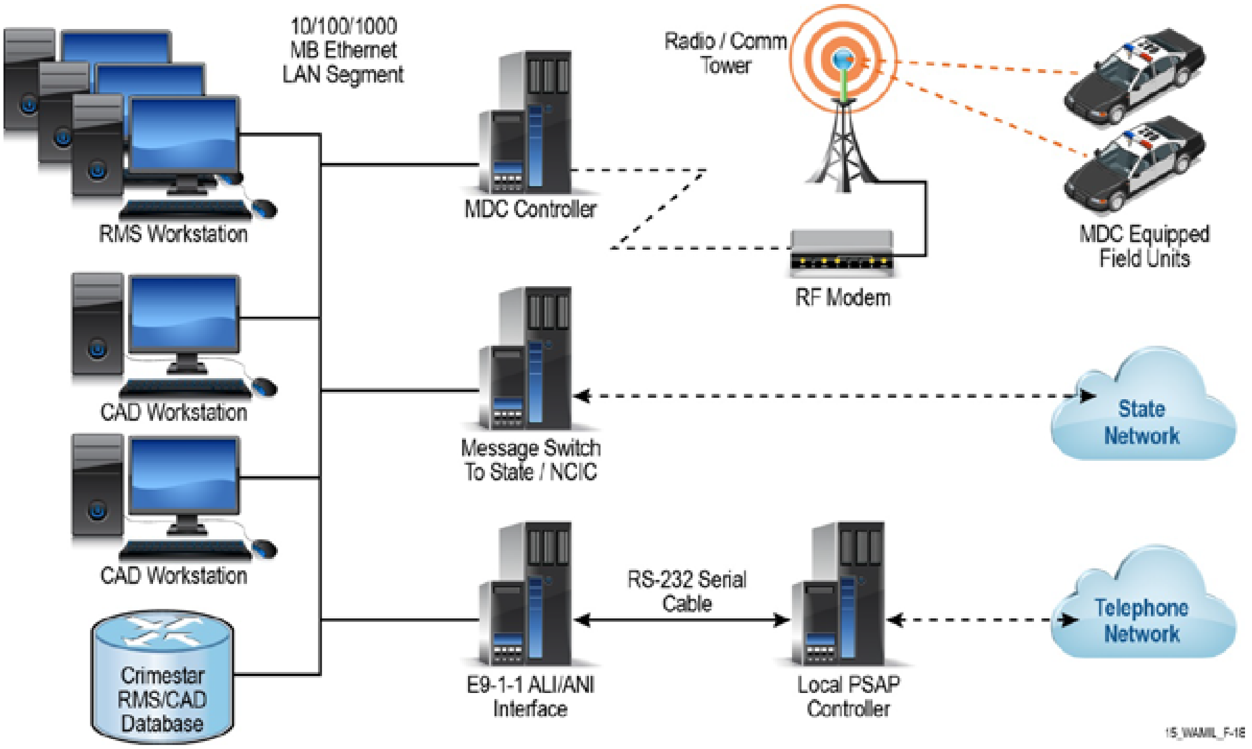
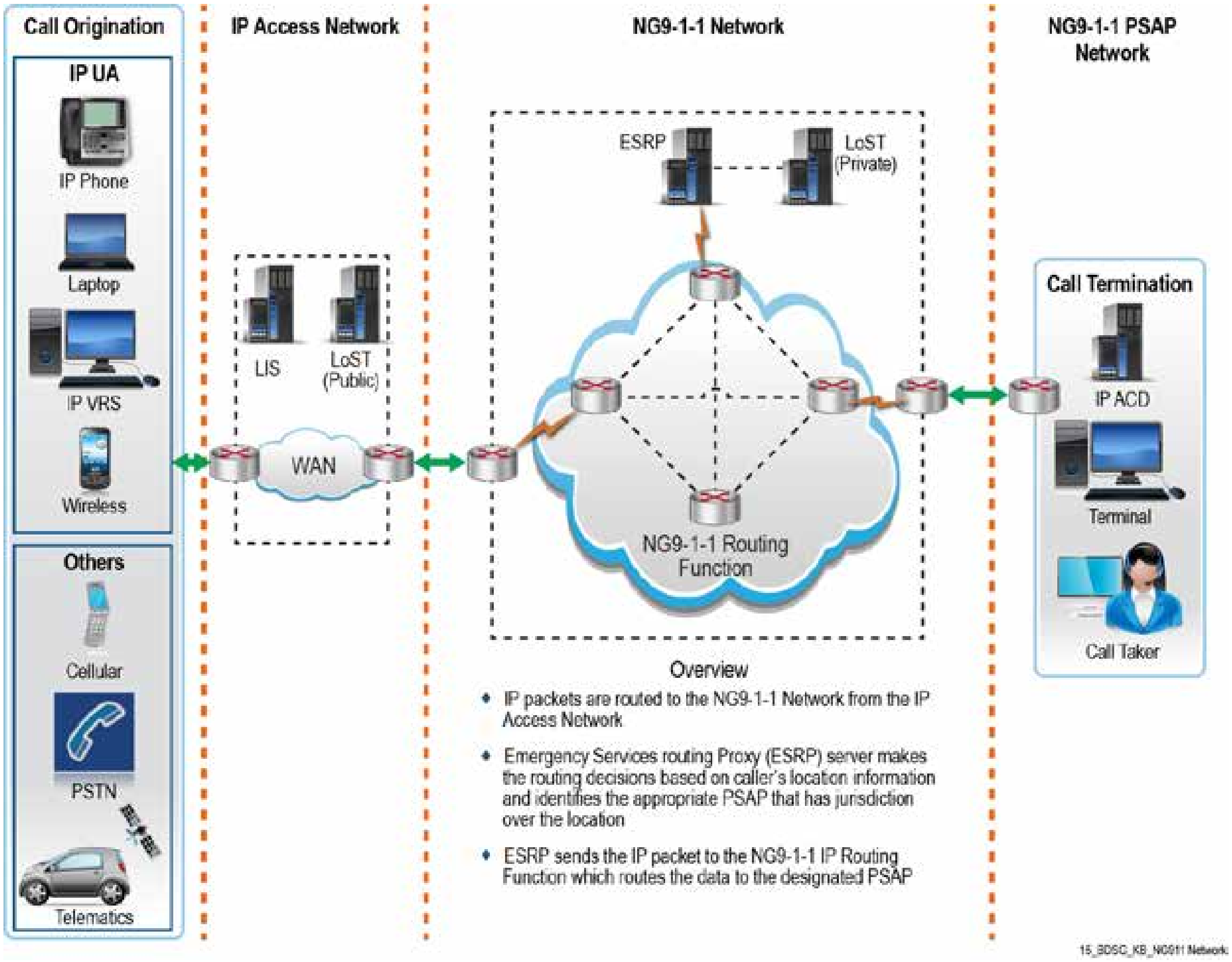


Exhibit 101. Typical PSAP Connectivity

We will connect at the LNG, SBC (BCF), or firewall to each of the state's networks, where today the session is converted from SIP to legacy support or, in the case of NG9-1-1, continues as SIP/i3 protocols into the PSAP. We will use multiple network scanning tools to identify machines and open ports on the network as well as determine which networks are interconnected. Data will be used to build out a network diagram for each of the PSAPs. For NG9-1-1 networks with connectivity to the ESInet, this connection will be verified and rules associated with the BCF and firewalls will be evaluated against NG-SEC and industry standards. Exhibit 102 below shows the ESInet connectivity.



- IP packets are routed to the NG9-1-1 Network from the IP Access Network
- Emergency Services routing Proxy (ESRP) server makes the routing decisions based on caller's location information and identifies the appropriate PSAP that has jurisdiction over the location
- ESRP sends the IP packet to the NG9-1-1 IP Routing Function which routes the data to the designated PSAP

Exhibit 102. ESInet Connectivity

2.3. External Network Security Assessment

Understanding an asset’s vulnerabilities begins with an external network security and vulnerability assessment to determine which hosts are visible outside the state of Alabama’s network. We will follow a penetration testing methodology for this security assessment but will halt prior to exploiting any of the target systems' vulnerabilities. We will use NG-SEC as a reference during our systems evaluations.

The intent of this first phase of the assessment is to identify flaws in security and systems configurations that may allow for unauthorized access to systems, data or applications.

Network discovery will focus on the external reconnaissance of the state's network to identify as many potential points of entry as possible. We will use various port scanning techniques to gather information from the state’s networks and individual IP addresses. These scans will provide information on ports, applications and other components of the systems that may be used for unauthorized access. Some of the tools we use include Hex Workshop, Hex-Rays IDA, Hex-Rays Decompiler, Core Impact Pro, Metasploit, Nessus, Burp Suite Pro, ActivePython, and Wireshark.

Once the hosts have been identified, we will ascertain ports that are exposed and services that are running. Network reconnaissance and service discovery from the vulnerability assessment will be used to move forward with identification and exploitation, where possible, during the penetration testing segment of the assessment. An external vulnerability assessment report will focus on the impact of potential external threats.

We will provide a list of systems to the state for evaluation and approval before any attempted penetration testing. Once these machines are identified, we will attempt to exploit these systems and obtain access to the host. We will attempt to establish a permanent presence on the IP address and then exploit that presence and network functionality to maneuver to new IP addresses. This testing will be accomplished both externally, as a potential hacker or malicious entity attempting to gain access to the state of Alabama's networks, and internally, as a simulated insider threat.

Exhibit 103 shows our methodology. The light blue boxes will be completed as part of the assessment. We will identify the networks and perform discovery using scanners and other tools. Our team uses the following exploitation frameworks during the validation process: scanners, disassemblers, fuzzing software, packet analyzers, web framework testers, database analyzers, and customized tools and scripts, as needed.

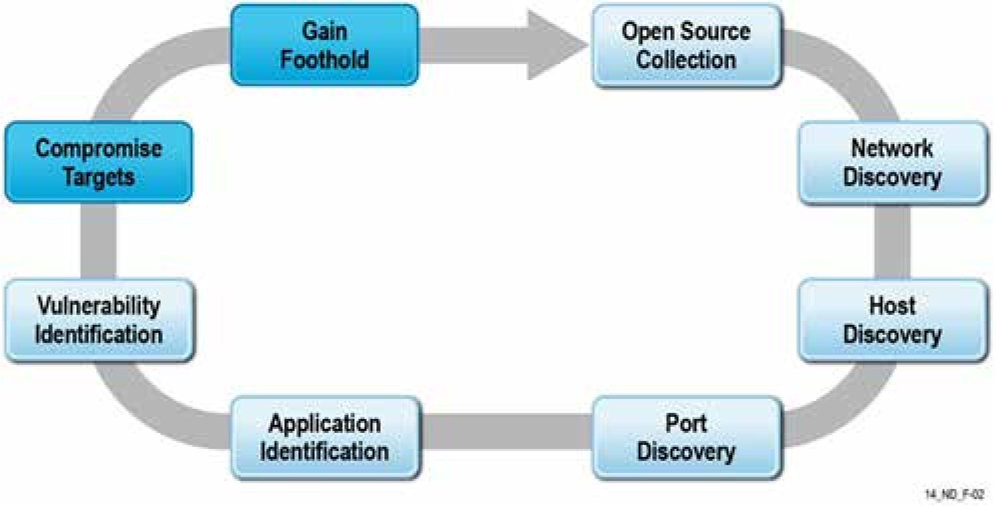


Exhibit 103. TCS Network Penetration Testing Methodology

We also will evaluate system configurations for potential unauthorized access to systems, data, or applications. Numerous port-scanning techniques will be used to gather information from the state of Alabama's networks and individual IP addresses. We will provide the state with a list of systems that may be at risk for evaluation in penetration testing. These systems, if approved by state personnel, will undergo additional penetration testing and evaluation for compromise and the ability to pivot to other parts of the network.

We will provide guidance to the state on vulnerability remediation and recommendations to strengthen the state of Alabama's security posture. Throughout this process, our team will take into consideration industry-standard recommendations to mitigate risks.

2.4. Internal Vulnerability Assessment

We will evaluate system configurations that may allow for unauthorized access to the state of Alabama's systems, data, or applications. This assessment simulates an internal authorized user to identify attack vectors on the network from a user with physical access to the state’s network, specifically its firewalls, switches, routers, Active Directory, VPN, and VoIP systems.

Various port-scanning techniques will be used to gather information from the state of Alabama's networks and its individual IP addresses. These scans will provide information on ports, applications, and other components of the systems that may be used for unauthorized access within the network. Following vulnerability assessment, we will provide a report detailing the hosts that may be vulnerable. The report will provide guidance on the Common Vulnerability Scoring System (CVSS) score used to determine the vulnerability as well as remediation guidance.

2.5. Web Application Security Assessment

We understand that the state could benefit from a web application security and penetration assessment. In contrast to network-based testing for known vulnerabilities, web application security assessment and penetration testing identify application design flaws resulting from the use of insecure coding practices or misconfiguration of the application and supporting services. Following testing, we will provide recommended methodologies for improving the security of web applications. Our methodology and approach to this assessment includes:

- Initial scoping
- Passive information gathering
- Vulnerability testing

Initial scoping will define the domains and pages to be tested as well as any authentication credentials that are required for the areas to be assessed.

In passive information gathering, we will manually interrogate the web application to understand the logic. Various tools like HTTP proxies will be used to gather information about the web applications and parameters of the HTTP pages.

Vulnerability testing will test the web app and web servers by adhering to Open Web Application Security Project (OWASP) recommendations and using the following criteria:

- Configuration management testing
- Business logic testing
- Authentication testing
- Authorization testing
- Session management testing
- Data validation testing
- DoS testing
- Web services testing
- Asynchronous JavaScript and XML (AJAX) testing

A detailed report associated with each finding, CVSS severity level, and remediation guidance will be provided to the appropriate state personnel.

2.6. Wireless Network Survey

Wireless networks are an extension of an organization’s infrastructure perimeter and should be tested thoroughly. Unsecured wireless networks expose organizations to the external world and pose a significant security risk. Rogue access points that do not follow the organization’s security guidelines, installed by employees on the infrastructure, also can be used to compromise an organization.

We will evaluate the wireless network with respect to the NENA NG-SEC guidelines in Section 6.4.6 and current industry best practices. This assessment would consist of a review of the wireless configuration policies of the network for state of Alabama-owned devices, password management, and change history. Site surveys will identify the wireless infrastructure, while wireless penetration tests will evaluate authentication controls for wireless users and the potential for unauthorized access to the wireless network. We will validate authentication controls for Alabama employees who attempt to gain unauthorized access and will determine the controls in place to identify physical tampering with wireless access points. We will perform a survey of any wireless 802.11 b/g/n networks found within the 2.4 and 5.8 GHz ranges. We will attempt to recover Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA)/Wi-Fi Protected Access II (WPA2) Pre-Shared Key (PSK) pass phrases. We will attempt to attack wireless devices by connecting as part of the preferred network list (PNL) and by setting up fake access point (AP) attacks, known as a man-in-the-middle assault. We will perform this assessment onsite at the state's offices.

2.7. Security Awareness Service

2.7.1. Security Awareness Training

TCS has extensive experience in developing and instructing security training to the United States military, Department of Defense (DoD), Fortune 500 corporations, and other large business enterprises. Our training portfolio spans from general employee security awareness training and chief information security officer (CISO) threat briefings to teaching more than 1,400 DoD/military cyber defenders on a yearly basis.

Our unique mission-oriented background, coupled with extensive university, public safety, large nonprofit, and enterprise-level security engagements, will prove to be extremely beneficial during the overall engagement and training of Alabama personnel and information technology personnel. NENA NG-SEC recommends security training for all employees on an annual basis. TCS security awareness training provides an innovative approach for implementing and maintaining an effective, measureable security awareness program that changes employee security behaviors.

Our security awareness training is an annual subscription implemented in 90-day iterations/plans. We will begin the subscription with a security awareness assessment, including an analysis of the organization’s security concerns and business needs. Each 90-day plan will outline the areas of focus and topics to be covered, as well as identify the most effective mediums (video, posters, campaigns, contests, demonstrations, briefings, etc.) and metrics to measure program effectiveness. The following collateral materials will create the most impact and therefore behavioral change; to implement this strategy, we will provide the following materials to implement this 90-day plan:

- A crafted kickoff email to all employees
- Three customized poster templates
- Three customized electronic display graphics
- Three customized newsletters
- Three customized screen savers
- Three customized lunch-and-learn presentations
- Four roadshow presentations (when applicable)
- Customized new employee training materials to implement into on-boarding
- Social engineering assessment at the beginning of each 90-day period.

2.7.2. Social Engineering Assessment

A social engineering assessment involves members of our team attempting to gain access to protected systems and data by impersonating state of Alabama employees or vendors, with contact made by phone, email, or in person. A social engineering assessment will test the physical controls around the facilities, networks, and confidential data. It is becoming increasingly common for attackers to exploit the human element of security. A social engineering assessment will identify areas of weakness in security controls and provide documented advice on remediation.

2.7.3. Methodology and Approach for Social Engineering Testing

We will work with the state of Alabama to define the targets, location, and method of social engineering to be employed. The end results can produce vital data for reducing risk.

Phishing—Phishing is an attempt to collect confidential information that will target users attempting to gain access to secure systems with information appearing to be from a trusted source. Phishing emails can be set up to entice an end user to provide information such as user name and password via a web form, or they can be configured to exploit the system's vulnerability when an email attachment is opened or a hyperlink is selected. We have the option to install an agent or just record the credentials of the phished user.

We can harvest a list of users from public sources or use a list provided by the state of Alabama. We recommend that approximately 25 percent of the user population be tested as a minimum sample. The state will be asked to approve the user pool list that will be part of the phishing attempt, as well as the content of the email, prior to the test launch.

Help Desk Calls—Supplied with an employee list, our team will contact the state of Alabama's help desk, posing as a state employee who is requesting a password reset. If successful, we will attempt to gain access to the reset account.

At the conclusion of this social engineering testing, we will be able to effectively answer the following questions:

- How effective is the state Alabama's security awareness training?
- How effective is the state's help desk security?
- What are the risks that confidential information can be leaked to unauthorized persons?

Detailed results, including the vulnerabilities present and/or exploited social engineering techniques such as email address of the user, IP address of the machine, and browser used to connect, will be identified. In addition to describing the current security posture, we will provide documented recommendations for improving security and reducing risk. Metrics from the assessment will drive areas covered in subsequent training.

2.8. Reporting and Debrief

During this final phase, we document all vulnerabilities and exposures within the state of Alabama's IT environment. Any vulnerability, exposure, or point of exploitation is thoroughly assessed before it is reported. This report aims to quantify exposures and identify how and why they may pose a risk to the state. Remediation recommendations on how to improve the state's security posture follow.

We will provide two reports to state personnel. We will provide preliminary draft findings to the technical point of contact for review and clarification. The final report will be issued after review and discussion are complete with the technical point of contact. A final presentation of the findings to the state of Alabama's executive team/Chief Information Officer (CIO) will be conducted in person to allow for information exchange and a thoughtful question-and-answer period.

Should we discover any findings of a critical nature (those that indicate past, current, or imminent breaches), we will stop testing and report what we have found immediately.

The first section of the report is targeted toward a nontechnical audience – senior management, auditors, board of directors, and other concerned parties. It contains:

- The executive summary.
- A summary of findings and recommendations that describe the environment and high-level findings and root causes, with recommendations based on potential risk to the state of Alabama.
- A remediation matrix prioritized based on severity of risk to business process.

The second section is targeted to technical staff and provides more granular detail:

- A summary of methods—Details specific to the engagement methodology.
- Detailed findings and recommendations—Details of any findings as well as recommendations for remediation. Evidence of controls and information sufficient to replicate the findings is included. Recommendations are based on these root causes and prioritized for a risk-based remediation with an estimation of relative work effort. Where strong controls in place have been identified, they are described along with their impact to the state of Alabama's security. Descriptions of techniques used and the causes of success or failure are detailed, as appropriate.
- Attachments—Details and specific examples, including screenshots, technical details, code excerpts, and other relevant observations. This section also contains data or documents that are relevant but do not fit in other categories.
- Remediation guidance—Details of how the state can improve its security posture from Day One following the submission of the report, including recommendations for hardware- and software-based solutions.

2.9. Protection of Information

We are committed to the protection of our information assets and those of our customers and partners. To that end, we have established an Information Security Policy to govern the protection of the information assets of our organization, customers, and suppliers from all threats, whether internal or external, deliberate or accidental, as well as to comply with all governing laws. The policy outlines the structure of the TCS Information Security Management System (ISMS), which is used to protect the information assets that reside within TCS, including information residing on the infrastructure and systems used to conduct business. We have been evaluated and certified for compliance with the ISO 27001 Information Security standard and remain committed to maintaining this registration.

As part of the planned Enterprise Security and Protection (ESP) Validation, we will have access to sensitive state of Alabama information. We will ensure the confidentiality of this information and will use ISO 27001 policies and procedures to safeguard the state's information assets.

2.10. Project Approach

We will provide evaluation services based on our proven approach and methodologies that are ISO 9001:2008 and ISO 27001 certified. The assessment will be conducted by a skilled team of assessors and penetration testers.

We will provide a kickoff meeting at the beginning of the network assessment and will provide an exit briefing for the state of Alabama upon completion of the field-work portion of the assessment.

2.10.1. Rules of Engagement

A critical component of our engagement is to clearly establish and agree to the rules of engagement. During our initial scheduling and kickoff sessions, the rules of engagement for the testing are established. Topics covered include:

1) Definition of scope
    a) Areas to be assessed – verification against the statement of work
    b) Verification of tools to be used
    c) Review of levels of effort for penetration testing and risk acceptance
2) Definition of any off-limit areas
    a) Critical network applications
    b) Declarations of known problems
    c) Web applications and web assessment scope
    d) Physical assessment scope
    e) Social engineering scope and determination if C-level personnel are to be included in the assessment
3) Written permission
    a) To engage in the assessment detailed in the statement of work
    b) If third-party components are to be assessed or hosted networks are used
        i) Notification of third party
        ii) Approval by third party for testing and any evaluation of applicable rules from the third party

   c) "Get out of jail free card" with appropriate signatures if physical assessment is planned
   d) If tools require connection to the auditee network, written permission should be obtained from CIO or higher

4) Verification of assessment timelines and schedule milestones
5) Verification reporting requirements, deliverables, timelines, and milestones
6) Definition of key personnel from the audit team and auditee team
   a) Roles and responsibilities
   b) Contact details
   c) Escalation rules – critical vulnerabilities should be reported within 24 hours of finding (provide example)
   d) Emergency planning

2.10.2. Project Timeline

We expect to be able to complete this assessment with approximately one week of time onsite, or remotely via VPN. Final report generation will take approximately one additional week.

2.11. Qualifications of Staff

Supporting and developing every facet of network operations, IT, and cybersecurity infrastructure, our Cyber Intelligence Group (CIG) draws from a deep pool of professional expertise. Several of the team's cybersecurity experts have been appointed to working groups of the FCC CSRIC, Maryland InfraGard, and the National Cybersecurity and Communications Integration Center (NCCIC).

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.

We have demonstrated success with executing large integration projects and global managed network solutions using established, industry-standard program management practices and effective, organized approaches for solution delivery. Our executive management team is committed to the success of this engagement and is assigning key personnel to support the Alabama program. A director-level PM has full authority to successfully execute the program and access to the critical resources required for successful implementation of the program.

Exhibit 104 shows the structure and staff for the program. Erik Wallace is the assigned Alabama project manager and the single point of contact for the program; he will work closely with Brad Hiner, the program manager of the Alabama ESInet program.

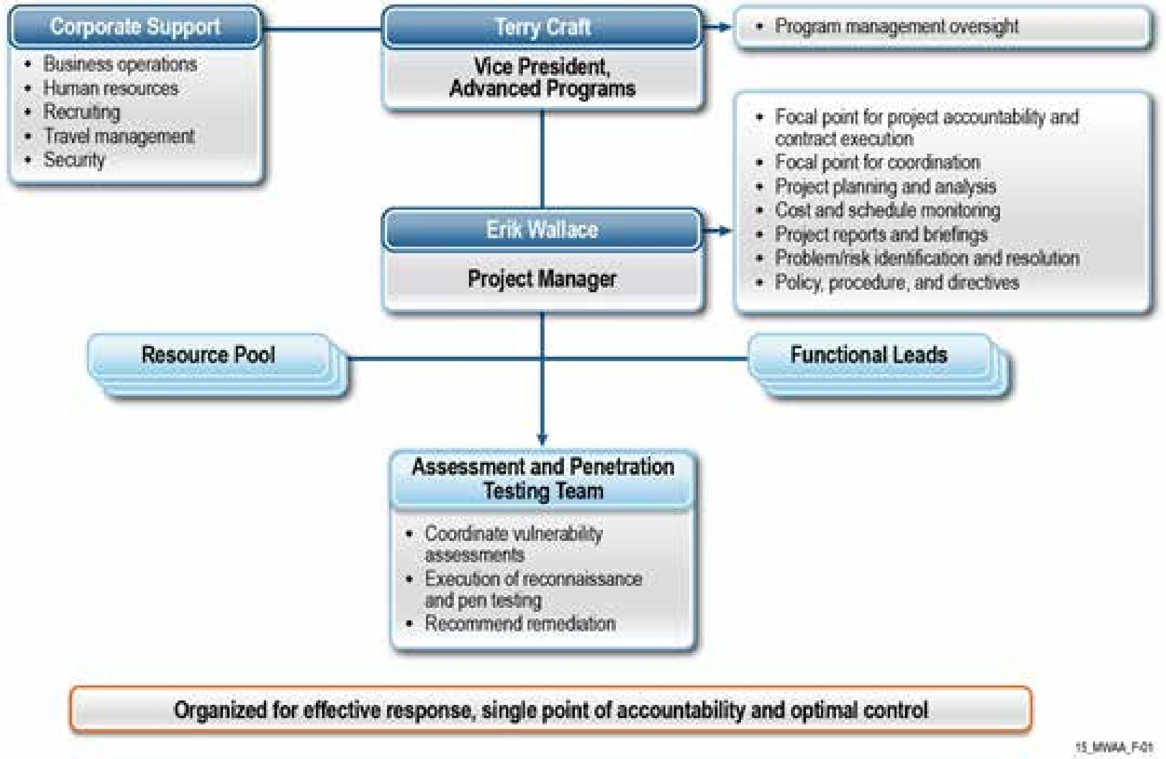

Corporate Support
• Business operations
• Human resources
• Recruiting
• Travel management
• Security
Terry Craft
Vice President, Advanced Programs
• Program management oversight
• Focal point for project accountability and contract execution
• Focal point for coordination
• Project planning and analysis
• Cost and schedule monitoring
• Project reports and briefings
• Problem/risk identification and resolution
• Policy, procedure, and directives
Erik Wallace
Project Manager
Resource Pool
Functional Leads
Assessment and Penetration Testing Team
• Coordinate vulnerability assessments
• Execution of reconnaissance and pen testing
• Recommend remediation
Organized for effective response, single point of accountability and optimal control
15_MWAA_F-01

Exhibit 104. Program Organization Chart

2.12. About TCS

TeleCommunication Systems, Inc. (TCS), a wholly-owned subsidiary of Comtech Telecommunications Corp., is a world leader in highly reliable and secure mobile communication technology. TCS infrastructure forms the foundation for market-leading solutions in E9-1-1, text messaging, commercial location, and deployable wireless communications. TCS is at the forefront of new mobile cloud computing services, providing wireless applications for navigation, hyper-local search, asset tracking, social applications, and telematics. Millions of consumers around the world use TCS wireless apps as a fundamental part of their daily lives. Government agencies use TCS' cybersecurity expertise, professional services, and highly secure deployable satellite solutions for mission-critical communications. Founded in 1987 by a U.S. Naval Academy graduate, TCS is U.S. owned and operated and headquartered in Annapolis, Maryland. TCS maintains technical, service, and sales offices throughout North America and the world.

The TCS CIG division delivers a host of cyber solutions to commercial and government agencies. TCS CIG helps harden highest-value entities, systems, and networks against cyber-attack. The group also offers a rigorous cybersecurity curriculum that provides comprehensive cybersecurity training to the DoD and commercial entities.

TCS currently has more than 1,100 employees across the United States and throughout the world. TCS conducts business through two operating segments: commercial (50 percent of 2014 revenue) and government (50 percent of 2014 revenue). Its customers include leading wireless and VoIP operators and carriers around the world, cable system operators, telematics vendors, public safety agencies, state and local governments, U.S. special operations and intelligence communities, and agencies of the U.S. Departments of Defense, State, Justice, and Homeland Security.

Market/Vertical Specializations

TCS' CIG has provided a variety of cyber solutions and services to commercial organizations and government agencies for the past 12 years. Each of our cyber experts has an average of 10 years of experience in providing cybersecurity operations, incident response, and security and risk assessment services. In addition, each year TCS teaches more than 2,000 military cyber operators the basics of network infrastructure as well as advanced cybersecurity skills.

Alabama Next Generation 9-1-1 Systems and Services

AL-NG911-RFP-16-001

Cost Proposal

March 4, 2016

Submitted to:

Leah Missildine
Interim Executive Director
Alabama 9-1-1 Board
Reference: AL-NG911-RFP-16-001
1 Commerce Street
Suite 610
Montgomery, AL 36104
334.440.7911
leah@al911board.com

Prepared by:

TCS TeleCommunication Systems
Enabling Convergent Technologies®

David Gleason
Regional Account Manager
TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401
802.473.2005
david.gleason@comtechtel.com
www.telecomsys.com

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®, 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™, 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 439 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.

Table of Contents

1. Introduction 1
2. Cost Savings Opportunities 2
3. Cost Proposal [RFP Attachment C] 3
4. Options 4
4.1. Migration of Wireline Carriers 4
4.2. Cybersecurity 4

Glossary

Term	Definition
AL9-1-1	Alabama 9-1-1 Board
CAMA	Centralized Automatic Message Accounting
ECRF	Emergency Call Routing Function

Term	Definition
GIS	Geographic Information System
LVF	Location Validation Function
TCS	TeleCommunication Systems, Inc.

1. Introduction

The Alabama Next Generation 9-1-1 Systems and Services RFP is a very detail-oriented articulation of NENA i3 compliance and functionality requirements. The pricing provided for the required solution is commensurate with the RFP full requirements. TCS has thoroughly analyzed the cost drivers and we recommend the areas outline in the Cost Savings Opportunities section as noteworthy cost reductions that can be gained in this proposal with modest adjustments or reductions to stated requirements.

2. Cost Savings Opportunities

- **Up to 3 Mbps PSAP network connection –** The TCS cost proposal includes a single network connection of 10 Mbps to each PSAP to meet RFP requirement 2.4.8.1. If the state were to deploy up to a 3 Mbps connection to each PSAP this would result in a savings of up to $469,000 recurring fees per year. Additional savings may be possible when actual site addresses are provided.
- **Removal of GIS based options, comprised of the following:**
  - Intrepid9-1-1 ECRF with GeoComm GIS managed services– Savings of $231,739 in non-recurring fees and $1,149,936 recurring fees per year. If this option is not deployed TCS will use tabular-based routing.
  - GeoComm LVF **–** Savings of $67,220 in non-recurring fees and $333,396 recurring fees per year.
- **EMedia™ –** If the state does not require a web-based text-9-1-1 browser this would result in a savings of $177,000 in non-recurring fees and $131,688 recurring fees per year.

3. Cost Proposal [RFP Attachment C]

A completed cost proposal spreadsheet is included in this submission.

4. Options

4.1. Migration of Wireline Carriers

Onboarding of existing wireline carriers to the TCS Intrepid9-1-1 NGCS base service. The current infrastructure, where the wireline carriers are delivering calls over Centralized Automatic Message Accounting (CAMA) trunks from the SRs, will be replaced with connections to the aggregation points in the ASA data centers. This would effectively be Phase 4 of the migration to the TCS service. TCS is happy to discuss this option with the state and negotiate applicable costs.

4.2. Cybersecurity

TCS will perform a comprehensive security assessment to examine Alabama’s ability to endure deliberate, malicious attempts to compromise its network.

State of Alabama

ALABAMA 911 Board AL-NG911-RFP-16-001

Attachment C Cost Proposal

AL-NG911-RFP-16-001

Attachment C – Cost Proposal

Table of Contents

Tab	Tab Name & Hyperlink
1	Title Page
2	Contents
3	Instructions
4	Instructions - Schedule 1
5	Schedule 1 – Equipment and Implementation
6	Instructions - Schedule 2-6 System Hosting
7	Schedules 2 - 6 – Service Operation

Note to Respondents: All pricing being sought under this RFP will be utilized to understand and evaluate your proposal.

AL-NG911-RFP-16-001
Attachment C – Cost Proposal
Instructions

Overview

Each respondent must complete the cost worksheets that follow, using the format as provided.   Please see the specific completion instructions included on each individual tab.

Respondents are encouraged to indicate if they are unable to provide specific products or services as the best and final offer process will define/refine the specific products and services required from the selected respondent.

Each respondent should document any and all assumptions used for arriving at cost estimates in the following sections.

The Cost Proposal categorizes unit pricing into two main groups: Implementation *(One time price)* and Recurring *(Monthly price)*. The Cost Proposal contains two sections. Section 1 is used for the functional components to implement and operate the 9-1-1 network and Sections 2-6 are specifically for hosted 9-1-1 services and operation.

The Cost Model is calculated from the Cost Proposal elements. Respondents do not need to develop a separate cost model.

Sample numbers have been placed into both the Cost Proposal spreadsheet as an illustration of how the spreadsheets work.

Respondents are expected to replace the sample numbers and modify the timeline to represent its proposal. These figures are not indicative of a possible budget.

RESPONDENTS ARE ADVISED THAT ALL ASSUMPTIONS MADE IN THE COST PROPOSAL AND ELSEWHERE IN THIS RFP REGARDING QUANTITIES (INCLUDING THE NUMBER OF PSAPS) ARE ESTIMATES ONLY,

SUCH QUANTITIES MAY INCREASE OR DECREASE. THE AGREEMENT IS FOR UNIT PRICES ONLY; AND WHERE APPLICABLE A MONTHLY RECURRING CHARGE FOR ONGOING OPERATIONS AND ADMINISTRATION.

OFFERORS, BY SUBMITTING THIS COST PROPOSAL, CERTIFY THAT THEY HAVE MADE A GOOD FAITH EFFORT TO ALLOCATE COSTS TO APPROPRIATE SERVICE CATEGORIES AND HAVE NOT ENGAGED IN UNBALANCED BIDDING OF ANY KIND.

Note to Respondents: All pricing being sought under this RFP will be utilized to understand and evaluate your proposal.   All pricing included in these schedules will be on a firm, fixed monthly recurring cost basis for the transfer, implementation, and on-going operations of the system.

Notes from the 911 Board: The solution(s) and services sought through this RFP may be proposed as an integrated, comprehensive solution, or as a stand-alone component representing a best in class service offering capable of being integrated with other components that will comprise the ANGEN ecosystem.

The Board may, at its discretion, integrate proposed solutions or components of proposed solutions in order to achieve an enterprise-wide, state-wide, best in class system that benefits all Alabama PSAPs and best serves the Board in fulfilling its duties under the law.

The Board would prefer an integrated solution with a designated primary vendor contractually responsible for providing the services as specified in this RFP.

The Board may, at its discretion, designate a contractual prime vendor and require contractual relationships, cooperative agreements, interconnection to and interaction with other system service providers or third parties as required or necessary for the operation of ANGEN

Schedule 1 will be used during the evalution to determine a one time cost; and monthly recurring cost that the AL911 Board will assume if the respondent is selected as the vendor. Schedule 1 also serves as a model for the implementation and monthly recurring costs. Respondents are responsible for ensuring the accuracy of the sub-totals of each section and the summation of the grand total at the bottom of Schedule 1.

Payment for Implementation and monthly recurring charges will be based upon a formula comprised of PSAP installation, ESInet operation, Wireless Call Volume delivered and Text services. The Board *will only pay* monthly recurring charges for services that have been *accepted and are documented as performing their intended function*. Respondents shall negotiate the graduated payment schedule with the Board during the transition and migration stage until reaching 100% of the proposed Monthly Recurring Charge.

AL-NG911-RFP-16-001
Attachment C – Cost Proposal
Instructions - Schedule 1

COST PROPOSAL:

This RFP calls for unit pricing by Deliverable / Cost Area. Respondent will insert its unit prices into the Cost Proposal spreadsheet. The columnar structure shall not be changed.

Implementation Pricing: Includes the Non-Recurring and one time charges for purchasing the equipment and facilities designed to provide the service functionality.

Recurring (Monthly) Pricing: Includes monthly Administration and Operations of the system, and Project Management charges for the duration of the projected implementation period.

The Project Management charge shall encompass all costs associated with implementation of the system and is the only allowable charge prior to acceptance of the ESInet and first PSAP.
Enter your recurring monthly charge for each of the following items:

AL-NG911-RFP ESInet Requirements

AL-NG911-RFP Specific Requirements

AL-NG911-RFP i3/NG Core Services Requirements

System Reporting and i3 Logging Requirements

Service and Support Requirements

Project Management and Planning Requirements

Electrical, Wiring and Cable Requirements

Other Required Items Charges - for items that the Vendor believes are needed but do not fit into one of the specified charge categories.
Please itemize any Other Required Items (add rows to spreadsheet if necessary)
At the bottom of the Cost Proposal spreadsheet please be sure to check and total all the monthly recurring charges.
An additional table is provided for System Hosting.
Please provide a monthly recurring cost for each of the two optional items.

Cost Proposal Column	Instructions
Deliverable / Cost Area	The Deliverable / Cost Area has been pre-populated with the anticipated components required to deliver 911 service to the Alabama PSAP's. Each of these components relates to an existing component or desired functionality. Respondents shall use the list as a guide to prepare unit costs for each functional element. The table includes a set of instructions to help guide how pricing information is entered into the table so that a detailed cost can be generated.
Estimated one time (Non- Recurring - NRC) start up costs, capitol costs etc.	The first three columns are used to enter Non-Recurring charges.
Unit of Measure	Unit of measure is a figure used to calculate a total Non-Recurring charge based upon a Unit cost. This may be a Primary PSAP ; one time implementation milestones; It is the respondents responsibility to articulate what measure they are using to calculate their costs
Estimated Cost	Estimated Cost is the cost of an individual component or system level functionality.
Extended Price (Unit of Measure x Estimated Cost)	The Extended price is a summation of the Unit of Measure multiplied by Estimated Cost.
Ongoing Monthly Recurring Charges (MRC)	Ongoing Monthly Recurring Charges are the monthly service fees billed to the AL911 Board by the system service provider.
Unit of Measure	Unit of measure is a figure used to calculate a total Non-Recurring charge based upon a Unit cost. Ongoing operational costs are expressed in terms of months, days or hours. It is the respondents responsibility to articulate what measure they are using to calculate their costs
Unit Price	Unit price is the monthly charge of a service function provided by the system service provider.
Extended Price (Unit of Measure x Unit Price)	Extended Price (Unit of Measure x Unit Price)

AL-NG911-RFP-16-001

Attachment C – Cost Proposal

Schedule 1 – Equipment and Implementation

This table indicates the pricing elements identified for requirements defined in AL-NG911 RFP ATTACHMENT D - Technical Specifications, for costs associated with the transfer, modification and implementation of the system (from date of contract execution to the end of the month statewide roll-out is completed). The successful Respondent is to group tasks/deliverables by the areas identified.

Instructions: Please fill in the cells shaded yellow. These items will be used to assign Cost components. Do not fill in the gray and blue cells. Note that the blue cells will populate automatically. Price example - ESInet configured at 8 PSAP's for a total of 80,0000. 8 is entered in the unit of measure, $10,000 entered in the estimated cost

	Estimated one time (Nonrecurring - NRC) start up costs, capitol costs etc.			Ongoing monthly recurring costs (MRC)		
Deliverable / Cost Area	**Unit of Measure**	**Estimated Cost**	**Extended Price (Unit of Measure x Estimated Cost)**	**Unit of Measure**	**Unit Price**	**Extended Price (QTY x Unit Price)**
Section 2 - ANGEN ESInet Requirements						
2.2 ANGEN ESInet Services		$ -	$ -	1	$ 19,135.00	$ 19,135.00
ESInet Deployment	1	$ 67,297.00	$ 67,297.00		$ -	$ -
PSAP IP Mesh Transport Network		$ -	$ -		$ -	$ -
IP Core Router Architecture (aggregation service routers)		$ -	$ -		$ -	$ -
Fiber to the PSAP (high availability option)		$ -	$ -		$ -	$ -
Commodity IP (tertiary service provider connections)		$ -	$ -		$ -	$ -
Regulatory and Legislative Support		$ -	$ -		$ -	$ -
2.3 ANGEN Architecture Requirements		$ -	$ -		$ -	$ -
2.4 ANGEN ESInet Features and Functions		$ -	$ -	118	$ 1,496.50	$ 176,587.00
2.5 ANGEN Network Failover		$ -	$ -		$ -	$ -
2.6 ANGEN Network Security		$ -	$ -		$ -	$ -
Sub-Total			**$ 67,297.00**			**$ 195,722.00**
Section 3 - ANGEN Specific Requirements						
3.1 System Service Provider Coordination Requirements		$ -	$ -		$ -	$ -
Legacy T-1 Network Transport (OSP to tandems)		$ -	$ -		$ -	$ -
Originating Service Provider Coordination (wireless carrier)		$ -	$ -		$ -	$ -
Orginating Service Provider Coordination (x-LEC)		$ -	$ -		$ -	$ -
Voice Message Services		$ -	$ -		$ -	$ -
Database Server and Software		$ -	$ -		$ -	$ -
pANI (psuedo ANI) and IP Provider ALI Records		$ -	$ -		$ -	$ -
Third Party Providers Interfaces (TCS and Intrado E2+ interfaces)		$ -	$ -		$ -	$ -
Inter-company ALI Server Connections		$ -	$ -		$ -	$ -
3.2 Interstate Interconnection Requirements		$ -	$ -		$ -	$ -
3.3 Text to 911 Requirements	118	$ 1,500.00	$ 177,000.00	118	$ 93.00	$ 10,974.00
Originating Service Provider coordination (wireless carrier)		$ -	$ -		$ -	$ -
Sub-Total			**$ 177,000.00**			**$ 10,974.00**
Section 4 - ANGEN i3 / NG Core Services Requirements						
4.1 NENA i3 Core Functional Requirements		$ -	$ -	1	$ 173,917.00	$ 173,917.00
SIP Gateway		$ -	$ -		$ -	$ -
SS7 Legacy Gateways		$ -	$ -	1	$ 11,083.00	$ 11,083.00
ALI Interface		$ -	$ -		$ -	$ -
IP Call Routing Platform	1	$ 167,000.00	$ 167,000.00	1	$ 31,254.00	$ 31,254.00
4.2 Border Control Function (BCF)		$ -	$ -		$ -	$ -
4.3 Emergency Call Routing Function (ECRF)	1	$ 231,739.00	$ 231,739.00	1	$ 95,828.00	$ 95,828.00
4.4 Emergency Services Routing Proxy (ESRP)		$ -	$ -		$ -	$ -
4.5 Legacy Network Gateway (LNG)		$ -	$ -		$ -	$ -
4.6 Legacy PSAP Gateway (LPG)	118	$ 544.00	$ 64,192.00	118	$ 93.00	$ 10,974.00
4.7 Legacy Selective Router Gateway (LSRG)* if included		$ -	$ -		$ -	$ -
4.8 Location Validation Function (LVF)	1	$ 67,220.00	$ 67,220.00	1	$ 27,783.00	$ 27,783.00
4.9 Legacy Database Services	1	$ 71,097.00	$ 71,097.00	1	$ 102,000.00	$ 102,000.00
4.10 Disaster Recovery / Business Continuity		$ -	$ -		$ -	$ -
Continuity of Operations (Resiliency)		$ -	$ -		$ -	$ -
Sub-Total			**$ 601,248.00**			**$ 452,839.00**
Section 5 - System Reporting and i3 Logging Requirements						

5.1 Reporting and Data Collection System Requirements	1	$ 223,000.00	$ 223,000.00	1	$ 66,067.00	$ 66,067.00
Remote Diagnostics		$ -	$ -		$ -	$ -
Performance Monitoring		$ -	$ -		$ -	$ -
Notification and Escalation		$ -	$ -		$ -	$ -
5.2 Statewide Statistical Monitoring		$ -	$ -		$ -	$ -
5.3 Operational Reporting and Logging		$ -	$ -		$ -	$ -
Logging Recording		$ -	$ -		$ -	$ -
System Reporting and Logging Requirements		$ -	$ -		$ -	$ -
5.4 Local Logging Recorder Interface		$ -	$ -		$ -	$ -
Sub-Total			**$ 223,000.00**			**$ 66,067.00**
Section 6 - Service / Support Requirements						
6.1 Customer Support Services		$ -	$ -		$ -	$ -
Network Operation, Administration and Management		$ -	$ -		$ -	$ -
PSAP Alerting and Remote System Status Alarming		$ -	$ -		$ -	$ -
Quality of Service (QoS) Monitoring and Reporting		$ -	$ -		$ -	$ -
Service Level Agreement (SLA) Monitoring and Reporting		$ -	$ -		$ -	$ -
Ongoing Development of New Public Safety Services		$ -	$ -		$ -	$ -
Spares		$ -	$ -		$ -	$ -
6.2 Help Desk		$ -	$ -		$ -	$ -
6.3 Trouble Handling and Ticketing Requirements		$ -	$ -		$ -	$ -
6.4 Training	1	$ 7,750.00	$ 7,750.00		$ -	$ -
6.5 Monitoring of Applications and Equipment		$ -	$ -		$ -	$ -
Intrusion Prevention and Detection		$ -	$ -		$ -	$ -
Identity and Access Management		$ -	$ -		$ -	$ -
6.6 Network Operations Center (NOC)		$ -	$ -		$ -	$ -
6.7 Alarm Categories		$ -	$ -		$ -	$ -
6.8 Scheduled Maintenance		$ -	$ -		$ -	$ -
Sub-Total			**$ 7,750.00**			**$ -**
Section 7 - Project Management and Planning Requirements						
7.1 Implementation Project Plan	1	$ 200,869.00	$ 200,869.00		$ -	$ -
Implementation Oversight		$ -	$ -		$ -	$ -
Cutover Planning		$ -	$ -		$ -	$ -
Migration Plan		$ -	$ -		$ -	$ -
7.2 System Test Plan		$ -	$ -		$ -	$ -
7.3 Transition Plan		$ -	$ -		$ -	$ -
7.4 Service Management Plan		$ -	$ -		$ -	$ -
Sub-Total			**$ 200,869.00**			**$ -**
Section 8 - Electrical, Wiring, and Cable Requirements						
8.1 Electrical					$ -	$ -
8.2 Electrical Interference		$ -	$ -		$ -	$ -
8.3 Wiring and Cabling	118	$ 600.00	$ 70,800.00		$ -	$ -
8.4 Grounding		$ -	$ -		$ -	$ -
8.5 Transient Voltage Surge Suppression		$ -	$ -		$ -	$ -
Sub-Total			**$ 70,800.00**			**$ -**
Total Transfer and Implementation Cost			**$ 1,347,964.00**			**$ 725,602.00**

Assumptions and Comments

2.2 ANGEN ESInet services: Cost shown includes rack space, power, cross connection/demarc extension, and power inverters for AC at the Huntsville and Montgomery data centers.

2.2 ESInet Deployment: Cost shown covers TCS deployment services to include: equipment ordering, staging/provisioning, installation oat the Huntsville and Montgomery data centers and equipment installation/turnup at the 118 PSAPs.

2.2 Fiber to the PSAP (high availability option): Requires more information to provide pricing. This was not listed in the technical proposal.

2.2 Commodity IP (tertiary service provider connections): Requires more information to provide pricing. This was not listed in the technical proposal.

2.4 ANGEN ESInet Features and Functions: Cost shown covers the 10 Mbps MPLS single circuit connection to each of the 118 PSAPs per RFP requirement 2.4.8.1. Refer to cost savings option noted in accompanying cost proposal document.

3.1 Legacy T-1 Network Transport (OSP to tandems): Requires more information to provide pricing for onboarding of existing wireline carriers.

3.2 Interstate Interconnection Requirements: This pricing is not included in the TCS cost proposal. Requires more information to provide pricing.

3.3 Text to 911 Requirements: Cost shown covers TCS deployment of EMedia™ service to the 118 PSAPs. This cost does not include Spanish language translation services which is billable at 6 cents per minute. Refer to cost savings option noted in accompanying cost proposal document.

4.1 NENA i3 Core Functional Requirements: The cost shown includes TCS Intrepid9-1-1 Next Generation Core Services to include: ESRP/PRF, LSRG and associated monitoring and managed services.

4.1 SS7 Legacy Gateways: The cost shown is the deployment of Sonus gateway equipment at the Huntsville and Montgomery AL data centers.

4.1 IP call routing platform: The cost shown is the deployment of the remaining Intrepid9-1-1 Next Generation Services hardware to be installed at the Huntsville and Montgomery AL data centers.

4.3 Emergency Call Routing Function (ECRF): The cost shown into deploy Intrepid9-1-1 ECRF and complimentary GeoComm GIS managed services. Refer to cost savings option noted in accompanying cost proposal document.

4.6 Legacy PSAP Gateway (LPG): The cost shown is to deploy two Mediant 1000 gateways with an FXS card in each chassis at the 118 PSAPs.

4.8 Location Validation Function (LVF): The cost shown is the cost to deploy GeoComm LVF. Refer to cost savings option noted in accompanying cost proposal document.

4.9 Legacy Database Services: The cost shown is to deploy Intrepid9-1-1 ALI and ongoing ALI database management by TCS AQPS team.

4.10 Disaster Recovery / Business Continuity: This pricing is not included in the TCS cost proposal. Requires site-specific criteria.

4.10 Continuity of Operations (Resiliency): This pricing is not included in the TCS cost proposal. Requires site-specific criteria.

5.1 Reporting and Data Collection System Requirements: The cost shown is to deploy ECaTS solution as described in Section 5 of the technical proposal.

6.4 Training: The cost shown is to provide TCS instructor led training services as described in requirement 6.4 of the technical proposal.

7.1 Implementation Project Plan: The cost shown is to provide the project management services as detailed in Section 8.1-8.3 of the technical proposal.

8.3 Electrical: The cost shown is to provide a 700VA UPS unit per PSAP rack.

8.4 Grounding: The proposed solution assumes a ground bar is available in the PSAP-provided equipment rack, capable of supporting additional external grounding cables.

AL-NG911-RFP-16-001

Attachment C – Cost Proposal

Instructions - Schedule 2-6 System Operation

Schedules 2 and 6 – System Hosting	Instructions
Schedule 2 On-going System Hosting Post Implementation from completion of statewide rollout Year 1	The Respondent(s) shall enter an annual price for the hosted services in the yellow shaded area. The sheet will calculate the extended price.
On-going System Hosting Post Implementation: Year 2	Same instructions as above
On-going System Hosting Post Implementation: Year 3	Same instructions as above
On-going System Hosting Post Implementation: Year 4	Same instructions as above
On-going System Hosting Post Implementation: Year 5	Same instructions as above
On-going System Hosting Post Implementation: Year 6 (Optional Extension)	Same instructions as above
On-going System Hosting Post Implementation: Year 7 (Optional Extension)	Same instructions as above
On-going System Hosting Post Implementation: Year 8 (Optional Extension)	Same instructions as above
On-going System Hosting Post Implementation: Year 9 (Optional Extension)	Same instructions as above
On-going System Hosting Post Implementation: Year 10 (Optional Extension)	Same instructions as above

AL-NG911-RFP-16-001
Attachment C – Cost Proposal
Schedules 2 - 6 – Service Operation

These schedules indicate the pricing for Respondents proposed services as defined in Attachment D for the ongoing hosting of the system starting the first full month after statewide roll-out is complete to the period ending five (5) years from contract execution and then for each of the five (5) annual renewal options.

Instructions: Please fill in the cells shaded yellow. These items will be used to assign Cost points. Do not fill in the gray and blue cells. Note that the blue cells will populate automatically. Example - Annual price of hosting service is $120,000 multiplied by 12 months - $1,440,000 total

Cost element	Annual price	Months	Total
Schedule 2 On-going System Hosting Post Implementation from completion of statewide rollout to the period ending Year 1	$ 725,602.00	4	$ 2,902,408.00
On-going System Hosting Post Implementation: Year 2	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 3	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 4	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 5	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 6 (Optional Extension)	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 7 (Optional Extension)	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 8 (Optional Extension)	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 9 (Optional Extension)	$ 725,602.00	12	$ 8,707,224.00
On-going System Hosting Post Implementation: Year 10 (Optional Extension)	$ 725,602.00	12	$ 8,707,224.00

Assumptions and Comments

TELECOMMUNICATION SYSTEMS, INC.

SECRETARY'S CERTIFICATE

The undersigned hereby certifies that he is the duly elected, qualified and acting Secretary of TeleCommunication Systems, Inc., a Maryland corporation (the "**Company**"), and that as such s/he is authorized to execute and deliver this certificate in the name and on behalf of the Company, and further certifies in his official capacity, in the name and on behalf of the Company, the items set forth below.

Dr. Stanton D. Sloane has been duly elected or appointed to the position of President and Chairman of the Board of Directors and is duly authorized to execute and deliver, in the name of and on behalf of the Company, any documents or other instruments, and to take all other actions that he may deem necessary, for the Company to submit its proposal, and if awarded the project based on such proposal to enter into a definitive contract, in connection with that certain AL-NG911-RFP-16-001 (as amended, the "RFP") issued by the Alabama 9-1-1 Board for Next Generation 911 Systems and Services, and the signature appearing opposite his name below is his genuine signature.

Name	Position	Signature
Dr. Stanton D. Sloane	President and Chairman of the Board of Directors	

IN WITNESS WHEREOF, the undersigned has hereunto set his hand as of this 1st day of March, 2016.

Patrick O'Hara

Name (print): Patrick O'Gara
Title: Secretary