

TU	Telematics Unit	
TVPA	Trafficking Victims Protection Act of 2000	
TVPRA	Trafficking Victims Protection Reauthorization Act of 2003	
TVSS	Transient Voltage Surge Suppression	
TVW	Testing Validation Worksheet	
TWC	Three-Way Calling	
UA	User Agent	
UAC	User Agent Client	
UAS	User Agent Service	
UBR	Unavailable Bit Rate	
UDDI	Universal Description, Discovery and Integration	
UDP	User Datagram Protocol	
UE	User Equipment	
UIM	User Identity Model	
UL	Underwriters Laboratories	
uLPN	Unique Local Public Safety Number	
UNI	Unbundled Network Interface	
UPS	Uninterruptible Power Supply	
URI	Uniform Resource Identifier	
URISA	Urban and Regional Information Systems Association	
URL	Uniform Resource Locator (location sensitive)	
URN	Uniform Resource Name (location insensitive)	
USAR	Urban Search and Rescue	
USF	Universal Service Fund	
USGS	United States Geological Survey	
USMC	United States Marine Corps	
USNG	United States National Grid	
USNO	United States Naval Observatory	
USPS	United States Postal Service	
USTA	United States Telephone Association	
USTSA	United States Telecommunications Suppliers Association	
UTC	Universal Coordinated Time	
UTRA	Universal Terrestrial Radio Access	
VBRnrt	Variable Bit Rate non-real time	
VBRrt	Variable Bit Rate real-time	
VC	Virtual Circuit	
VCI	Virtual Circuit Identifier	
VCIN	Violent Crime Information Network	
VCO	Voice Carry Over	
VDB	Validation Data Base	
VDSL	Very high-speed Digital Subscriber Line	
VE2	Voice over Internet Protocol E2 Interface	

VEDS	Vehicle Emergency Data Sets	
VEP	VoIP End Point	
VESA	Valid Emergency Services Authority	
VF	Validation Function	
VFG	Virtual Facility Group	
VI	Video Interpreter	
VIN	Vehicle Identification Number	
VLAN	Virtual LAN	
VLR	Visitor Location Register	
VoATM	Voice over ATM	
VoDSL	Voice over Digital Subscriber Link	
VoFR	Voice over Frame Relay	
VoIP	Voice over Internet Protocol	
VON	Voice over Network	
VoP	Voice over Packet	
VPC	VoIP Positioning Center	
VPI	Virtual Path Identifier	
VPN	Virtual Private Network	
VRI	Video Remote Interpreting	
VRS	Video Relay Service	
VSP	VoIP Service Provider	
W3C	World Wide Web Consortium	
WAENS	Wide Area Emergency Notification System	
WAN	Wide Area Network	
WAP	Wireless Access Point	
WCM	Wireline Compatibility Mode	
WFS	Web Feature Service	N
WG	Working Group	
WGS 84	World Geodetic System 1984	
WiFi®	Wireless Fidelity	
WiMAX	Worldwide Interoperability for Microwave Access	
WNC	Wireless Network Controller	
WPS	Wireless Priority Service	
WSDL	Web Service Definition Language	
WSP	Wireless Service Provider	
WSS	Web Services Security	
WTSC	Wireless Technologies and Systems Committee	
WWW	World Wide Web	
XACML	eXtensible Access Control Markup Language	
XML	eXtensible Markup Language	
XMPP	eXtensible Messaging and Presence Protocol	N
XSD	W3C XML Schema Definition	

XXXXX	Indicates an error or mistake in typing (erasing the error)	
--------------	---	--

NG9-1-1 System and PSAP Operational Features and Capabilities Requirements



NENA NG9-1-1 System and PSAP Operational Features and Capabilities Requirements
Document 57-750, v1 (Draft), March 2, 2011
Standards Advisory Committee Approval Date, March 2, 2011
NENA Executive Board Approval Date, June 14, 2011

Prepared by:
National Emergency Number Association (NENA) Operations Committee NG Requirements Work
Group

Published by NENA
Printed in USA



NENA
OPERATIONS REQUIREMENTS DOCUMENT

NOTICE

This Operations Requirements Document (ORD) is published by the National Emergency Number Association (NENA), and is intended to be used by Standard Development Organizations (SDO) including NENA, and/or designers and manufacturers of systems that are used for the purpose of processing emergency calls. It should be considered to be a source for identifying the requirements necessary to meet the needs of the emergency services industry as it applies to the subject covered in this ORD. It is not intended to provide complete design specifications or parameters for systems that process emergency calls.

NENA reserves the right to revise this ORD for any reason including, but not limited to, conformity with criteria or standards promulgated by various agencies, utilization of advances in the state of the technical arts or to reflect changes in the design of network interfaces or services described herein. It is possible that certain advances in technology will precede any such revisions. Therefore, this ORD should not be the only source of information used.

Patents may cover the specifications, techniques or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document is not to be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics. NENA recognizes that the requirements listed here may never be satisfied by products or services from any single source.

This document has been prepared solely for the use of Standard Development Organizations (SDO) and/or designers and manufacturers of systems that are used for the purpose of processing emergency calls, as well as E9-1-1 Service System Providers, network interface and system vendors, participating telecommunications companies, etc.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Operations Committee has developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association

4350 North Fairfax Drive, Suite 750

Arlington, VA 22203

800-332-3911 or

opsdoccomments@nena.org

Acknowledgments:

The National Emergency Number Association (NENA) Operations Committee NG Requirements Work Group developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

Version 1, Approval Date, 06/14/2011

Members	Company/Agency
Pete Eggimann-ENP, Operations Committee Chair	Metropolitan Emergency Services Board (MN)
Wendi Lively-ENP, Operations Committee Vice Chair	Spartanburg County Communications, SC
Rick Jones-ENP	NENA
Steve O’Conor-ENP	NENA
John Haynes-ENP	Chester County, PA
Stephen Wisely	APCO
Kathy McMahon	APCO
Marc Berryman-ENP	Digital Data Technologies, Inc.
Barb Thornburg-ENP	NENA

This committee would also thank Pete Eggimann, ENP, Wendi Lively, ENP and Rick Jones, ENP for their support and assistance.

TABLE OF CONTENTS

1 EXECUTIVE OVERVIEW..... 6

2 INTRODUCTION..... 7

2.1 OPERATIONS IMPACTS SUMMARY 7

2.2 TECHNICAL IMPACTS SUMMARY 7

2.3 SECURITY IMPACTS SUMMARY 7

2.4 DOCUMENT TERMINOLOGY 7

2.5 REASON FOR ISSUE/REISSUE..... 7

2.6 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK 8

2.7 DATE COMPLIANCE 8

2.8 ANTICIPATED TIMELINE..... 8

2.9 COST FACTORS 8

2.10 FUTURE PATH PLAN CRITERIA FOR TECHNICAL EVOLUTION 8

2.11 COST RECOVERY CONSIDERATIONS..... 9

2.12 ADDITIONAL IMPACTS (NON COST RELATED) 9

2.13 INTELLECTUAL PROPERTY RIGHTS POLICY 9

2.14 ACRONYMS/ABBREVIATIONS 10

3 CALL DELIVERY 12

3.1 CALL QUEUE MANAGEMENT 12

3.2 CALL DISTRIBUTION RULES..... 12

3.3 USE OF CALL TYPE INFORMATION..... 14

3.4 CALL TREATMENT RULES..... 16

3.5 CALL AUTHENTICATION 17

4 CALL PROCESSING 18

4.1 CALL ANSWERING 18

4.2 COMMUNICATIONS PATH..... 19

4.3 CALL ASSESSMENT 21

4.4 EMERGENCY RESPONSE LOCATION 21

4.5 MOBILE CALLER LOCATION 22

4.6 EMERGENCY RESPONDER DETERMINATION..... 23

4.7 MULTIPLE COMMUNICATION DEVICE SUPPORT..... 24

4.8 ADDITIONAL DATA..... 26

4.9	DATA TRANSFER.....	27
4.10	LOCATION MAP DISPLAY.....	27
4.11	WORKING WITH GIS DATA.....	28
4.12	CALL HANDLING PROTOCOLS AND PROCEDURES.....	29
5	CALL MANAGEMENT.....	30
5.1	CALL DETAIL RECORDS.....	30
5.2	INCIDENT RECORDS.....	30
6	LOGGING.....	31
6.1	CALL LOGGING.....	31
7	LOCATION AND ROUTING DATABASE MANAGEMENT.....	33
7.1	CALL DATA ERROR CORRECTION.....	33
7.2	LOCATION VALIDATION.....	34
8	RECOMMENDED READING AND REFERENCES.....	34
9	EXHIBITS.....	35
10	PREVIOUS ACKNOWLEDGMENTS.....	35



1 Executive Overview

Significant work is currently underway to enable the 9-1-1 system to transition from telephone-based voice only systems to a fully interoperable Internet Protocol (IP) based, multimedia Next Generation 9-1-1 (NG9-1-1) system capable of supporting a variety of different communications devices and protocols. This document contains a list of operational capabilities or features that are expected to be supported in a standards-based NG9-1-1 system. The capabilities described within this document represent minimum levels of required functionality. These capabilities should be developed around common, standard IP-based messaging and telecommunications interfaces to allow interoperability between the NG9-1-1 system and public telecommunications systems, regardless of vendor or service provider. Nothing in this document should be interpreted as limiting the development of additional capabilities or features by 9-1-1 equipment and software developers.

This document is intended to be a guide for the NENA Technical and Operations Committees, as well as other national and international standards organizations, to use in developing and finalizing standards in preparation for implementation of standards-based NG9-1-1 systems. The IP network, 9-1-1 equipment, software vendors, as well as service providers should use this requirements document as a guide during their product research and development. PSAP administrators may also find this document useful for planning purposes, as they prepare to transition from their current 9-1-1 system to NG9-1-1 systems, and to update internal policy and procedures to leverage the new features, requirements, and capabilities in the NG environment.

The current 9-1-1 network uses technology that, without conversion, is not compatible with many digital forms of telecommunications technology that are now being widely deployed. The rules and assumptions under which the current 9-1-1 systems were built are no longer valid (such as Service Providers who no longer are physically based in the locality where service is provided and aren't even licensed telephony providers, nomadic customers, mobile customers, and dramatic changes associated with numbering resources to name a few). This has led to degradation in the enhanced 9-1-1 service now provided to the general public. The NG9-1-1 systems will support the communications protocols and devices now in common use by the general public.

NG9-1-1 systems implemented at the regional, state, or multi-state level, will offer more opportunities to share infrastructure, resources, work load, and call-related data throughout the 9-1-1 call / public safety response continuum. PSAP operations will no longer need to be tied to a specific geographic location / building, but can be distributed over a wide area as long as there is connectivity to the system. This will allow all PSAPs, regardless of size, to have access to any and all applications on the NG9-1-1 system and permit ubiquitous deployment of NG systems to happen more rapidly than has been possible by anything requiring an individual PSAP by PSAP deployment.

NG9-1-1 systems will give PSAPs the ability to work together cooperatively in ways that the current systems do not allow, including interoperability between other PSAPs, response agencies, and applications; as well as improved disaster recovery options. NG9-1-1 systems will allow

PSAPs to receive call-related data from multiple data sources such as telematics service providers, wireless carriers, or Internet based telecommunications service providers. NG9-1-1 systems will support voice, text, images, and video, giving more emergency communications alternatives for the hearing impaired or disabled community (i.e. text messaging, video relay services, etc.) as well as the general public.

2 Introduction

2.1 Operations Impacts Summary

As new implementations of NG9-1-1 systems become more widely available, this document will be updated to provide additional guidance in developing operational guidance.

2.2 Technical Impacts Summary

9-1-1 Authorities will become more involved in implementing and managing NG9-1-1 systems which will allow PSAP managers to concentrate on actual call handling and response. Proper call routing in NG9-1-1 systems will be geo-based, and will require 9-1-1 Authorities to provide accurate GIS information related to PSAP and responder service areas, preferably on a regional or statewide scale. IP-based 9-1-1 equipment and software at the PSAP will rely on network and data technical standards in order to take full advantage of the IP environment and ensure true interoperability throughout the entire 9-1-1 system at a regional, state, national, and international level. Commonly used Internet-based telecommunications, messaging, image, and video protocols and standards will need to be supported in order to maintain interoperability with Internet applications. NG9-1-1 system minimum quality of service (QoS), redundancy, and diversity standards will need to be established to ensure system reliability.

2.3 Security Impacts Summary

Acknowledgement of Security Standards, Guidelines and best practices is of vital importance when planning and implementing new Operations and Features. Use of the NENA Security for Next Generation 9-1-1 Standard (NG-SEC) NENA 75-001, Version 1, February 6, 2010, is required.

2.4 Document Terminology

The terms "shall", "must" and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "desirable" or "preferably".

2.5 Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Version	Approval Date	Reason For Changes
Original	02/01/2005	Initial Document
2	[MM/DD/YYYY]	Update to 58-001 to clarify Operations NG9-1-1 Requirements

2.6 Recommendation for Additional Development Work

As new implementations of NG9-1-1 systems become more widely available, this document will be updated to assist in developing additional operational guidance.

2.7 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application.

To ensure true compliance, the manufacturer shall upon request, provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945 or equivalent.

2.8 Anticipated Timeline

Not applicable

2.9 Cost Factors

9-1-1 Authorities that work together to implement NG9-1-1 systems at the regional, state, or multi-state level will need to work out funding agreements that may be significantly different from how current 9-1-1 systems are funded. Who has responsibility for a particular NG9-1-1 system function, system operations/management, system security, participant call volume, and how any surcharges or other taxes are collected will all be factors in funding the NG9-1-1 system.

2.10 Future Path Plan Criteria for Technical Evolution

In present and future applications of all technologies used for 9-1-1 call and data delivery, it is a requirement to maintain the same level or improve on the reliability and service characteristics inherent in present 9-1-1 system design.

New methods or solutions for current and future service needs and options should meet the criteria below. This inherently requires knowledge of current 9-1-1 system design factors and concepts, in order to evaluate new proposed methods or solutions against the Path Plan criteria.

Criteria to meet the Definition/Requirement:

1. Reliability/dependability as governed by NENA’s technical standards and other generally accepted base characteristics of E9-1-1 service



2. Service parity for all potential 9-1-1 callers
3. Least complicated system design that results in fewest components to achieve needs (simplicity, maintainable)
4. Maximum probabilities for call and data delivery with least cost approach
5. Documented procedures, practices, and processes to ensure adequate implementation and ongoing maintenance for 9-1-1 systems

This basic technical policy is a guideline to focus technical development work on maintaining fundamental characteristics of E9-1-1 service by anyone providing equipment, software, or services.

2.11 Cost Recovery Considerations

While specific cost recovery options are beyond the scope of this document, the use of IP technology may allow 9-1-1 to be another application on a shared public safety IP infrastructure. This could allow cost recovery to be considered on a wider scale than a 9-1-1 specific cost recovery model. NG9-1-1 system routing functions could also be used to support other N-1-1 entities that need accurate call routing, which could broaden the funding base and add additional funding sources.

2.12 Additional Impacts (non cost related)

The requirements contained in this NENA document are expected to have impacts regarding 9-1-1 management. Documents building on these requirements should provide additional details and guidance.

2.13 Intellectual Property Rights Policy

NENA takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:

National Emergency Number Association
4350 N Fairfax Dr, Suite 750

Arlington, VA 22203-1695

800-332-3911

or: opsdoccomments@nena.org

2.14 Acronyms/Abbreviations

Some acronyms/abbreviations used in this document have not yet been included in the master glossary. After initial approval of this document, they will be included. See NENA 00-001 - NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents.

The following Acronyms are used in this document:		
<i>Acronym</i>	<i>Description</i>	** N)ew (U)pdate
<i>ACD</i>	Automatic Call Distribution, Automatic Call Distributor	
<i>GIS</i>	Geographic Information System	
<i>IP</i>	Internet Protocol	
<i>IP PSAP</i>	Internet Protocol Public Safety Answering Point	N
<i>NG9-1-1</i>	Next Generation 9-1-1	
<i>ORD</i>	Operations Requirement Document	N
<i>PSAP</i>	Public Safety Answering Point or Primary Public Safety Answering Point	
<i>PSTN</i>	Public Switched Telephone Network	
<i>QoS</i>	Quality of Service	
<i>SOP</i>	Standard Operating Procedures	
<i>VoIP</i>	Voice over Internet Protocol	

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	** N)ew (U)pdate

The following Terms and Definitions are used in this document:		
<i>Term</i>	<i>Definition</i>	<i>** N)ew (U)pdate</i>
<i>Call</i>	A session established by signaling with two way real-time media and involves a human making a request for help. We sometimes use “voice call”, “video call” or “text call” when specific media is of primary importance. The term “non human initiated call” refers to a one-time notification or series of data exchanges established by signaling with at most one way media, and typically does not involve a human at the “calling” end. The term “call” can also be used to refer to either a “Voice Call”, “Video Call”, “Text Call” or “Data-only call”, since they are handled the same way through most of NG9-1-1.	N
<i>Incident</i>	A real world occurrence such as a heart attack, car crash or a building fire for which one or more calls may be received.	
<i>Next Generation 9-1-1 (NG9-1-1)</i>	http://www.nena.org/sites/default/files/NG9-1-1%20Definition%20Final%201.1.pdf The above link will take you to the web page showing NENA’s current description/definition of NG9-1-1.	
<i>System</i>	A system is the hardware, software and databases necessary for NG9-1-1.	N

3 Call Delivery

3.1 Call Queue Management

(Provide the capability to manage call queues and deliver the call to the call taker queue.)

- A. Call queues shall be displayed only to authorized system users.
- B. The call queue information shall be based on the information delivered with the call.
- C. The system shall provide the capability to configure the call queue content, based on local policy rules.
- D. The system shall provide the capability to intelligently monitor call queues and automatically take action based on local policy rules.
- E. The system shall provide real-time updates to the call queue.
- F. The system shall be capable of providing a dynamically updated, incident specific voice announcement to callers in queue based on policy rules.
- G. The system shall display the time elapsed for each call in the queue.
- H. The system shall display call queues by an automatic call distributor type of function group.
- I. The system shall display the time a call was placed in queue.
- J. The system shall be capable of providing a visual warning when a call remains unanswered after a predefined number of seconds, as defined in local policy rules.
- K. The system shall be capable of providing an audible warning when a call remains unanswered after a predefined number of seconds, as defined in local policy rules.
- L. The system shall utilize location information delivered with the call and allow an automatic call distribution type of functionality to dynamically change call processing based on local policy rules.
- M. The system shall support assignment of calltakers to geographic zones that correspond to incoming location information of the call.
- N. The system shall analyze geographic information and alert calltakers when calls outside of a particular geographic area are presented.
- O. The system shall support assignment of calls by calltaker skill sets based on an automatic call distribution type of function, based on the available calltaker skill set.

3.2 Call Distribution Rules

(Create specialized calltaker groups to be used in conjunction with call distribution rules)

Note: The term automatic call distribution refers to the ability for Policy Based Routing of incoming requests. This function should not be confused with the legacy product called ACD.

- A. An automatic call distribution type of function group is a queue of calls/events defined by local policy rules such as call types, call data, call location and input from caller, providing skill-based call routing to a defined group of calltakers.
- B. The system shall provide the capability to create groups with an automatic call distribution type of function.
- C. The system shall support multiple groups with an automatic call distribution type of function.
- D. The system shall provide the capability to read groups with an automatic call distribution type of function.
- E. The system shall provide the capability to update groups with an automatic call distribution type of function.
- F. The system shall provide the capability to suspend groups with an automatic call distribution type of function.
- G. The system shall provide the capability to delete groups with an automatic call distribution type of function.
- H. The system shall provide the capability to assign a calltaker to a group or groups with an automatic call distribution type of function by calltaker training level, skill, and experience level.
- I. The system shall provide the capability to assign multiple calltakers to a group with an automatic call distribution type of function.
- J. The system shall provide the capability to add calltakers to a group with an automatic call distribution type of function from a remote location.
- K. The system shall provide the capability to add calltakers to a group with an automatic call distribution type of function who are not physically located in a PSAP.
- L. The system shall provide the capability to delete calltakers from a group with an automatic call distribution type of function from a remote location.
- M. The system shall provide the capability to restore groups with an automatic call distribution type of function.
- N. The system shall provide the capability to save groups with an automatic call distribution type of function.
- O. The system shall provide the capability to dynamically support all of the automatic call distribution type of function listed.

- P. The system shall provide the capability to create automatic call distribution type of functions.
- Q. The system shall provide the capability to read automatic call distribution type of functions rules.
- R. The system shall provide the capability to update automatic call distribution type of functions rules.
- S. The system shall provide the capability to delete an automatic call distribution type of functions rule.
- T. The system shall provide the capability to suspend an automatic call distribution type of functions rule.
- U. The system shall provide the capability to restore an automatic call distribution type of functions rule.
- V. The system shall provide the capability to assign automatic call distribution type of function groups to a call distribution rule.
- W. The system shall provide the capability to define automatic call distribution type of function rules based on resource availability, resource ability, group, event type, and direct number identification.
- X. The system shall provide the capability to distribute automatic call distribution type of function rules.
- Y. The system shall provide the capability to dynamically support all of the automatic call distribution type of function rules listed.

3.3 Use of Call Type Information

(Receive and validate call type information (e.g., vehicle telematics, silent alarm) from communications devices and recalculate call type and default priority based on supporting data.)

- A. The system shall use call data to perform call treatment.
- B. The system shall use the following data to determine Call Type: Emergency Location and Additional Data associated with the call.
- C. The system shall be able to detect any unrecognizable formats or garbled data in the Call Type.
- D. The system shall validate incoming Call Type.
- E. The system shall provide the capability to allow a system administrator to create new Call Type definitions.

- F. The system shall provide the capability to allow a system administrator to update Call Type definition.
- G. The system shall ensure that the incoming call matches a predefined Call Type.
- H. The system shall provide the capability to allow a system administrator to read an expected Call Type definition.
- I. The system shall provide the capability to allow a system administrator to delete Call Type definition.
- J. The system shall provide the capability to allow a system administrator to save Call Type definition.
- K. The system shall assign a default Call Type for calls received with an undefined Call Type.
- L. The system shall determine an appropriate Call Type for calls received with an undefined Call Type.
- M. The system shall assign a default Call Type for calls received with an unrecognizable Call Type.
- N. The system shall record the original Call Type when a received call type is a) unrecognizable, b) undefined.
- O. The system shall indicate to the calltaker whether the Call Type of a call was changed by the system as the result of a received undefined Call Type.
- P. The system shall indicate to the calltaker whether the Call Type of a call was changed by the system as the result of a received unrecognizable Call Type.
- Q. The system will check Additional Data associated with the call to determine if the Call Type or Priority needs to be updated.
- R. The system shall determine if Additional Data is associated with the call.
- S. The system shall identify how to access the Additional Data.
- T. The system will be able to retrieve any Additional Data.
- U. The system shall maintain the credentials to allow access to the Additional Data associated with the call.
- V. The system shall be able to automatically retrieve or query data from Additional Data sources to obtain the Additional Data associated with the call.
- W. The system shall be able to automatically process the retrieved data and make a decision on whether or not to change the Call Type or Priority, based on policy rules.

- X. The system will be able to update the call detail record with all data that affects the call treatment, and shall include the pointer(s) (e.g., reference – URL) to the datasets that provided the additional information.

3.4 Call Treatment Rules

(Route call from the initiator and call-originating service to the appropriate destination based on identified call treatment including location information received (civic or geographic/geodetic.)

- A. The system shall route calls based on the associated call treatment process in the policy rules.
- B. The system shall be able to handle calls that involve error cases (e.g. garbled callback or no location data), based on policy rules.
- C. The system shall determine the call treatment for each call based on call type, location, and policy rules.
- D. The system shall determine the proper treatment for fragmented or incomplete call records.
- E. The system shall send a status/acknowledgement message to the communications device based on identified call treatment (e.g. text message returned saying “we got your text”)
- F. The system shall be able to provide an alternate call treatment when a call cannot be immediately answered because of call volume
- G. The system shall provide the capability for the network administrator to dynamically make changes to the policy rules (which determine next-hop routing).
- H. The system shall support the ability to establish a pre-determined limit on the total number of simultaneous 9-1-1 calls presented to the PSAP, regardless of what technology was used to deliver each individual call; and, at the option of the PSAP, when the pre-determined limit has been reached, provide alternate call treatments. (i.e., flexible queuing, network busy signal or message, interactive voice response, rollover to an alternate PSAP, etc.)
- I. The system shall be designed with sufficient bandwidth to support the predetermined limit of simultaneous calls using the type of transport technology supported that has the highest bandwidth requirement (e.g. calls may be voice, video, and / or text, with additional multimedia attached).
- J. The system shall be able to overflow 9-1-1 calls directly to another designated PSAP, or multiple PSAPs, using agreed upon, predetermined criteria at both the sending and receiving PSAPs, including the receiving PSAP’s total call load.
- K. The system shall be capable of providing alternate call treatment for potentially redundant calls within a dynamically defined geographic area. Potentially redundant calls are those calls that may be reporting the same high visibility incident at a location, (e.g. highway crash).

- L. The system shall provide alternate call treatment capability including distribution to an alternate location, a pre-recorded message that includes the ability to transfer to another location, a fast-busy signal, and other predefined call treatment or combination of treatments.
- M. The system shall provide alternate call treatment capabilities for all media types or combination of media types including incoming voice, video, text, and emergency event notification (sensors / alarms) calls.
- N. The system shall provide a visual indication, at the original PSAP, that calls are overflowing.
- O. The system shall provide a visual indication at the designated overflow PSAPs or the alternate locations that they are now receiving overflow calls from the original PSAP with identification of the originating PSAP.
- P. It shall be possible for PSAPs to accept additional media (e.g. images) from callers.
- Q. The system shall be capable of multiple, pre-set failover scenarios.
- R. The system shall allow PSAPs to receive event notifications from authorized systems.
- S. The system shall support the generation of event notifications through standard interfaces of event notification systems operated by authorized entities within the NG9-1-1 system.
- T. The system shall support the use of a backup PSAP that may or may not be on the same Emergency Services IP Network as the failed PSAP.
- U. The system shall support emergency call routing from any entity capable of initiating an emergency call.
- V. The system shall permit a call, and all of the associated call data, to be "quarantined" if a computer virus or some other malicious code is detected by the system's security systems.
- W. The calltaker must be permitted to communicate with a quarantined caller to determine if an actual emergency exists.

3.5 Call Authentication

(The call authentication process ensures that the appropriate entity, such as the originating provider or other responsible party, has been granted permission to proceed (call treatment/processing) after call has accessed/entered the system.)

- A. The system shall create a call detail record as the call enters the system.
- B. The system shall write the certificate authentication details (successful and failed) to the call detail record.

- C. The system shall certify / authenticate that the originating provider or other responsible party has been granted permission to deliver calls.
- D. The system of authenticating provider certificates shall be deployed with strong authentication (RSA-1024 or better, as documented in RFC2313 [14]) using X.509 certificates and Certificate Revocation Lists as profiled in RFC 3280 [15] and best current practice. (08- 001)
- E. The system shall not accept calls from un-certified or unauthenticated providers (beyond this initial Step), the originating provider or other responsible party shall generate a call refusal or error message for the user (e.g., voice recording) if the call is not successfully authenticated.
- F. The system shall generate a notice when the call is successfully authenticated.

4 Call Processing

4.1 Call Answering

(Provide the capability to answer a 9-1-1 call)

- A. The system shall provide the capability for a calltaker to select a call from a call queue.
- B. The system shall permit an authorized calltaker, as defined in local policy rules, to select any call from the queue.
- C. The system shall record the time when a calltaker has selected a call.
- D. The system shall record and identify the calltaker who selected the call.
- E. The system shall record when a calltaker has selected a call out of queue order.
- F. The system shall permit the calltaker to indicate a status of “Not Ready” for the situation where the user is signed-on (but not available to answer queue calls). – Based on local options include the ability to show not ready status to supervisor and other calltakers.
- G. The system shall provide the capability to answer an incoming call.
- H. The system shall be configurable to automatically answer the call for the calltaker.
- I. The system shall display the default call handling procedure based on the data available with the call.
- J. The system shall provide the capability to place a call on hold (two-way mute – audio specific).
- K. The system shall provide the capability for calltaker to activate one-way mute for call. The system shall display a time on hold alert after predetermined number of seconds. This

should display to the calltaker placing it on hold and/or the appropriate supervisor, based on local policy rules.

- L. The system shall be capable of displaying call detail record of an active call and displaying multiple active call detail records of calls being worked, based on local policy rules.
- M. The system shall be configurable to specify the elapsed time before the “time on hold” alert will be generated.
- N. The system shall be configurable to deliver an audible and/or visual alert when the “time on hold” alert has been generated.
- O. The system shall provide the capability to take a call off hold.
- P. The system shall record and log the time a call is placed on hold.
- Q. The system shall record and log the time a call taken off hold.
- R. The system shall re-read and redisplay the call detail record each and every time a call is taken off hold.
- S. PSAPs shall have facilities to detect and react to silent calls
- T. The system shall be capable of terminating all communication links associated with the call.
- U. The system shall have the capability to park a call.
- V. The system shall have the capability to notify the caller that their call has been parked.

4.2 Communications Path

(Establish communications path between call)

- A. The system shall provide the capability to reestablish a call path to a communications device.
- B. The system shall provide the capability to establish a call path between a calltaker and a communications device if a call is abandoned before a calltaker can answer the call.
- C. The system shall provide the calltaker with the supported call back communications method(s) for each call.
- D. The system shall provide the option to read from the call detail record data to display any Additional Data that exists that provides additional call back methods.
- E. The system shall display the supported call back communications methods to the calltaker, when a call back has been requested.
- F. The system shall permit the calltaker to select from the supported communications methods when initiating a call back.
- G. The system shall store the results of the call back attempt.

- H. It shall be possible for PSAPs to supply ring back media to callers.
- I. Voice activity Detection shall be disabled for emergency calls.
- J. The system shall support the option of maintaining connectivity with the caller's device in situations of premature disconnect by the caller, when the originating network supports that feature.

4.3 Call Assessment

(Determine the nature of the emergency and provide an initial assessment of the situation)

- A. The system shall display call handling procedures to a calltaker.
- B. The system shall provide the capability to document the nature of the emergency for each call.
- C. The system shall provide the capability to update the nature of the emergency.
- D. The system shall provide the capability to document additional information for a call.
- E. The system shall allow the call taker to edit information they are manually entering during the event creation process. Once the event is created all of the information must be preserved and any subsequent changes or editing must be logged.

4.4 Emergency Response Location

(Determine whether an emergency is located at the caller's location or elsewhere. Ensure responders are directed to the correct location.)

- A. The system shall display call location information to the calltaker.
- B. The system shall provide the capability to customize the display rules for call locations.
- C. The system shall display call locations based upon display rules.
- D. The system shall be capable of identifying known locations, or landmarks, within a user defined radius of geo-coordinates.
- E. The system shall be capable of converting call location from civic address to geographic coordinates.
- F. The system shall validate all locations entered by the calltaker.
- G. The system shall provide the capability to document incorrect location information for correction, in the standard formats.
- H. The system shall provide the calltaker with a capability to document the actual location of the emergency.
- I. The system shall provide the capability to append the caller location information to the call detail record as the emergency location.
- J. The system shall provide the capability for the calltaker to search for the emergency location using: geographic coordinates, civic address location, by clicking a location on an interactive map display, landmarks / common place names.
- K. The system shall display location search results to the calltaker.

- L. The system shall provide the capability for the calltaker to select the emergency location from the location search results.
- M. The system shall write the emergency location to the call detail record when the calltaker accepts an alternate location as the emergency location.
- N. The location source shall be identified and should be verified.
- O. The system shall be capable of supporting three-dimensional location information (longitude, latitude, altitude).

4.5 Mobile Caller Location

(Receive location information for mobile callers; Wireless, mobile VoIP, and related technologies)

- A. The system shall provide the capability to automatically update the caller location, as specified in policy rules.
- B. The system shall provide the capability to activate the automatic location update function on a call-by-call basis.
- C. The system shall also provide capability of requesting updated caller location from a mobile call service provider at a predetermined and configurable number of seconds.
- D. The system shall be capable of providing alerts to calltaker when caller location has changed, subject to local policy rules.
- E. The system shall provide the capability for a calltaker to manually initiate a location update.
- F. The system shall provide the capability for the calltaker to manually initiate continuous location updates, at provider-defined update intervals.
- G. The system shall archive automatic location updates as part of the Call.
- H. The system shall archive manual singular location updates as part of the Call.
- I. The system shall archive manual continuous location updates as a part of the Call so the entire location history can be reconstructed.
- J. The system shall support the displaying of any location information present in the PIDF-Lo.
- K. The system shall provide the capability to display update request results on the map display.
- L. The system shall notify the calltaker before displaying automatic rebid requests.
- M. The system shall support the capability of requesting different location types (last known, current, new, etc.)
- N. The system shall support the capability of varying location parameters (maximum location age, minimum confidence factor, etc.) in the request for location updates.

- O. The system shall support, if supplied, additional location related parameters such as velocity and direction, and be able to present those to the call taker.
- P. The system shall determine, based on call and additional information received, if location updates are supported for the call.
- Q. The system shall provide an indication to the call taker whether or not location updates are supported for the call.

4.6 Emergency Responder Determination

(Select appropriate emergency responder agencies (based on the nature and location of emergency, incident management procedures, and standard operating procedures (SOP))

- A. The system shall display the recommended emergency responder agencies associated with the emergency location.
- B. The system shall display the recommended emergency responder agencies associated with the caller location until the emergency location is available.
- C. The system shall display the recommended emergency responder agencies associated with the nature of emergency.
- D. The system shall display the recommended emergency responder agencies associated with the call data if nature of emergency is not available.
- E. The system shall log the displayed responder agencies for each call.
- F. The system shall display call handling procedures based on policy rules to the calltaker.
- G. The system shall display the mode of communication capabilities of the displayed responder agencies.
- H. The system shall contain Responding Agency Data.
- I. The Responding Agency Data shall include the following information for all responding agencies in the PSAPs jurisdiction: agency name, type of agency, response area, URL, telephone number, available communications media.
- J. The system shall be capable of displaying the recommended responder agencies associated with the nature of event as determined by local policy rules.
- K. All emergency responder agencies shall be uniquely identifiable nationwide.
- L. The system shall have the capability to access individual agent data within the responding agency data.
- M. The system shall contain SOPs for the display of emergency responder agency information.

- N. The system shall contain rules for automatically determining whether a calltaker is needed for a given call based on data with the call or the type of device (i.e. data only sensor) placing the call.
- O. The system shall provide the capability to refresh the list of response agencies.
- P. The system shall provide the capability to search the responder list.
- Q. The system shall provide the capability to search the responder list using Boolean search terms.
- R. The system shall provide the capability to select responders from the list.
- S. The system shall provide the capability to select individual agents within a responding agency.
- T. The system shall log the selected responder agencies for each call.
- U. The system shall provide the capability to provide a call record and associated notes to the selected responder agencies' dispatchers (all available data, the call itself – text voice video – and any calltakers notes associated with the call).
- V. The system shall be capable of receiving the location of the caller from the access network or from a 3rd party.

4.7 Multiple Communication Device Support

(Establish communication between multiple communications devices; call taker, caller, third-party (e.g., vehicle telematics) service provider, and appropriate public safety entities)

- A. The system shall provide the capability to establish a call path to a communications device.
- B. The system shall provide the capability to establish a call path between multiple communication devices.
- C. The system shall identify the media type of an incoming call (voice, video and/or text) to the calltaker when accepting or placing a call.
- D. The system shall provide the capability to establish multi-media conferencing.
- E. The system shall provide the ability to query a national database for emergency provider contact methods and access data, such as third party call centers, transportation dispatch centers.
- F. The system shall log the results of the conference or transfer attempt.
- G. The system shall provide the capability to store frequently used conference call participant paths.

- H. The system shall provide the capability to store frequently used communications device paths.
- I. The system shall choose the most appropriate conference type based on media and/or data of the call.
- J. The system shall be capable of establishing conferences with any type of multimedia from any device capable of calling 9-1-1.
- K. The system shall log conference requests, including: time/date, all conference participants, conference type, and conference status.
- L. The system shall alert the calltaker in the event of a successful conference setup.
- M. The system shall alert the calltaker in the event of an unsuccessful conference setup.
- N. The system shall provide the capability to identify all conference parties.
- O. The system shall provide the capability to allow all conference parties to identify all conference parties.
- P. The system shall provide the capability to conference requested parties into a conference call.
- Q. The system shall provide the capability to automatically connect multiple parties based on call data, access rights, and local policy rules.
- R. Information maintained or collected by any party shall be accessible to all other authorized parties on the call. All authorized parties shall receive notification of available data.
- S. The system shall be capable of utilizing a secondary network.
- T. The system shall be capable of dynamically switching between primary and secondary networks to ensure call quality.
- U. The system shall provide the capability of muting parties, including partial mute of individuals, being conferenced/transferred.
- V. The system shall provide the capability of each calltaker to mute, un-mute other conference parties.
- W. The system shall provide the capability to perform intra-PSAP call transfers
- X. The system shall provide the capability to transfer calls to legacy PSAPs and legacy emergency responder agencies.
- Y. The system shall notify the call taker of the incapacity/limitations of a targeted destination PSAP or emergency responder agency in supporting a call or data transfer (e.g., transferring an RTT call to a legacy emergency responder agency)

4.8 Additional Data

(Obtain Additional Data after call delivery to facilitate call processing.)

- A. The system shall determine which queries are authorized for access based on established policy rules.
- B. The system shall record the query parameters for all queries performed in the call detail record database.
- C. The system shall record the query results for all queries performed in the call detail record database.
- D. The system shall determine which queries are automatically executed based on established policy rules.
- E. The system will provide an indicator that Additional Data is available. Additional Data should be accessible via a standard process involving no more than three steps, such as mouse clicks.
- F. The system shall be capable of acquiring all Additional Data associated with the call and making it accessible to the calltaker, subject to security access and local policy rules.
- G. The system shall provide the capability for authorized personnel to access Additional Data associated with the call.
- H. The system shall provide the capability to search Additional Data associated with the call.
- I. The system shall display Additional Data associated with the call based on policy rules.
- J. The system shall support queries of Additional Data associated with the call from other internal and external systems (SIP messages, SIP header, call detail record data, floor plans, medical records data, and other data sources).
- K. The system shall support drill-down queries of Additional Data associated with the call to obtain additional detail.
- L. The system shall be capable of allowing a PSAP to download Additional Data from an external source for fast retrieval under specifically agreed to conditions.
- M. The system shall require that all Additional Data elements provide data elements associated with the location, caller or call.
- N. The system shall be capable of acquiring Additional information from other databases and sources based on the location of the call or the location of the emergency location.

- O. The system shall be capable of distinguishing between data associated with a building or campus and a tenant of such a building or tenant. Each source may have different Additional Data.
- P. The system shall be capable of providing Additional Data associated with the Address of Record of the caller.

4.9 Data Transfer

(Transfer all Additional Data associated with the call and any manually-entered data (e.g. call taker notes) concerning the call to the appropriate responding agency dispatch or other authorized entity.)

- A. The system shall provide the capability to transfer a call, additional call related data received or a query key for the retrieval of the additional data, call related data created during call processing (e.g. call taker notes), and the call detail record.
- B. The system shall provide the capability to transfer the call and the associated data only to authorized recipients.
- C. The system shall log the transfer of all calls and associated data.
- D. The system shall log data transfer attempts, including transfer request date/time, notification of transfer success/failure date/ time, transfer requestor, intended recipient, transferred data.
- E. The system shall display a message that data was not received to the originating requestor upon failed call data transfer.
- F. The system shall display an acknowledgement message of data receipt to the originating requestor upon successful call data transfer.
- G. The system shall provide the capability to convert the NG9-1-1 location information to meet the capability of the destination PSAP.

4.10 Location Map Display

(Display location and geospatial information on a GIS based map display)

- A. The system shall provide the capability to display GIS based data.
- B. The system shall provide capability to display a Caller Location on a GIS map display.
- C. The system shall provide the capability to display an Emergency Location on a GIS map display.
- D. The system shall be capable of displaying multiple locations associated with a single call by using different icons to represent the locations.
- E. The system shall provide the capability to zoom on the GIS based map display.
- F. The system shall provide the capability to pan on GIS based map display.

- G. The system shall provide the capability to store geographic information system databases in GML formats.
- H. The system shall provide the capability to turn on and off specific theme based layers of information, and be able to select on specific layers on a GIS map display (e.g. water, hydrants, city boundaries, aerial photography).
- I. The system shall provide the capability to display the emergency responder agencies associated with a Caller Location on the GIS based map display.
- J. The system shall provide the capability to display the emergency responder agencies associated with an Emergency Location on the GIS based map display.
- K. The system shall display the emergency responder agencies associated with a Caller Location on the GIS based map display.
- L. The system shall display the emergency responder agencies associated with an Emergency Location on the GIS based map display.
- M. The system shall display caller location information on the GIS based map display.
- N. The map display shall have the ability to include both raster and vector data.
- O. The GIS based display shall include status and selected call data and any associated data through indicators as part of the call or emergency location status icons.

4.11 Working with GIS Data

(Manipulate location and geospatial information)

- A. The system shall provide the capability to manipulate the GIS based map display.
- B. The system shall provide the capability to draw geometric shapes on the GIS based map display.
- C. The system shall provide the capability to select data from the drawn geometric shapes on the GIS based map display.
- D. The system shall provide the capability to search the NG9- 1-1 data by any selected geometric shape drawn on the GIS based map display.
- E. The system shall provide the capability to search the NG9- 1-1 data repositories by any user generated geometric shape.
- F. The system shall provide the capability to display query results on the GIS based map display.
- G. The system shall display the emergency responder agency for a given location.

- H. The system shall have the capability of displaying any information in the databases associated with any locations on the GIS based map display, where such information is not restricted by security or policy.

4.12 Call Handling Protocols and Procedures

(Ensure proper and efficient call handling and compliance with PSAP processes and best practices through the creation and automation of protocols and procedures).

- A. The system shall display call handling procedures to a calltaker.
- B. The system shall provide the capability for authorized personnel to edit call handling procedures.
- C. The system shall provide the capability for authorized personnel to suspend call handling procedures.
- D. The system shall provide the capability for authorized personnel to input and edit call handling procedures.
- E. The system shall log all changes made to call handling procedures including unique user id, time, and audit trail of changes made.
- F. The system shall provide the capability for authorized personnel to delete call handling procedures.
- G. The system shall provide the capability for authorized personnel to amend and notate any compliance reports and the system will log any changes.
- H. The system shall provide the capability to measure a calltakers consistency with a call handling procedure.
- I. The system shall provide the capability to generate statistical or call specific reports of a calltaker's consistency with call handling procedures.
- J. The system will be able to generate statistical or call specific reports based on authorized personnel defined reports.
- K. The system shall provide the capability for a calltaker to select the appropriate call handling procedure based on the data associated with the call.
- L. The system shall store the data that measures the compliance of each calltaker.
- M. The system shall provide the capability to read the data that measures the compliance of each calltaker to authorized individuals.
- N. The system shall provide the capability to sort the data that measures the compliance of each calltaker.

If the system has call handling protocol software, the following requirements apply:

1. The system shall provide the capability for a calltaker to select pre-arrival instruction based on the nature of the emergency.
2. The system shall display pre-arrival instructions to the calltaker.
3. The system shall prioritize pre-arrival instructions based on data delivered with the call, additional information obtained, or information associated with the call, by the calltaker.
4. The system shall provide the capability to search the pre-arrival instruction database.
5. The system shall provide the capability to deliver appropriate pre-arrival instructions in accordance with accepted standards and operational best practices.

5 Call Management

5.1 Call Detail Records

(Dynamically create, maintain and preserve Call Detail Records)

- A. The Call Detail Record shall at minimum contain: date(s), times, packetized Additional Data, service originator code, Caller Location, Call Type, network processing data, caller classification, and all other data added by the system during the call processing from originator to call conclusion.
- B. The system shall provide the capability to create a Call Detail Record.
- C. The system shall provide the capability to read a Call Detail Record.
- D. The system shall provide the capability to update a Call Detail Record with any updates being logged, including transitions, which will include time stamp and user ID.
- E. The system shall provide the capability to delete a Call Detail Record for the purpose of archiving.
- F. It shall be possible to uniquely identify a call throughout its life cycle in the call detail record.

5.2 Incident Records

(Dynamically create, maintain and preserve Incident Records)

- A. The system shall provide the capability to create an Incident Record.
- B. The system shall provide the capability to read an Incident Record.
- C. The system shall provide the capability to update an Incident Record.
- D. The system shall provide the capability to delete an Incident Record.
- E. The system shall assign a unique identifier to an Incident Record.

- F. The system shall provide the capability of merging 2 or more Call Detail Records to an existing Incident record.
- G. This merging may be done after the call(s) have been completed, such as by records management staff assigned with this responsibility.
- H. The system shall permit the appropriate entity/person(s) to be assigned the capability of determining which existing Call Detail Record will be the master one.
- I. The system shall provide the capability to search Incident Records.
- J. The system shall store Incident Records.
- K. The system shall maintain the association between an Incident Record, the Call Detail Record, and Call Recording, including notes added by the call taker.

6 Logging

(Preserve a detailed record of the interactive communications occurring during a call.)

6.1 Call Logging

- A. The system shall log all calls.
- B. The system shall provide the capability to log calls at redundant, diverse locations.
- C. The system shall log all incoming multimedia, data, and designated non-emergency communications.
- D. The system shall link logged data with the unique identifier of each call.
- E. The system shall be able to link logged data regardless of media type to construct a single logged record of all data associated with a call or incident.
- F. The system shall provide the capability to transfer a logged data to an external source.
- G. The system shall provide the capability to transfer selected components of the logged data set based on the third party's level of authorization.
- H. The system shall be capable of indicating call termination
- I. The system shall be capable of logging which party terminated the call.
- J. The system shall provide the capability to access logged data from a remote location.
- K. The system shall log calls while the call is in a call queue, assigned, in process, and on hold.
- L. The system shall provide the capability to access logged data.
- M. The system shall provide the capability to display previous logged data for Instant Playback based on established local policy.

- N. The system shall provide the capability to retrieve a logged data with its Call detail Record.
- O. The system shall provide the capability to search the logging system database.
- P. The system shall provide the capability to retrieve logged data based upon search criteria.
- Q. The system shall provide the capability to retrieve logged data after a call.
- R. The system shall provide the capability to retrieve logged data during a call.
- S. The system shall provide the capability to monitor logged data during a call.
- T. The system shall provide the capability to display non-audio logged data
- U. The system shall provide the capability to replay logged data regardless of media type.
- V. The system shall provide the capability to pause logged data.
- W. The system shall provide the capability to rewind logged data.
- X. The system shall provide the capability to fast forward logged data
- Y. The system shall provide the capability to locate an incident and all its related calls within the logging function.
- Z. The system shall support validation and credentialing of authorized IP connections for logging and associated functions.
- AA. The Logging function shall support Audio mixing (combining of multiple audio streams into a single stream for playback, i.e. bridging).
- BB. The Logging function shall support playback of multiple video streams simultaneously.
- CC. The Logging function shall support Simultaneous display and/or playback of Logged Data such that the original timing of the Logged Data is reproduced in the original sequence.
- DD. The Logging function shall support Retrieval of Logged Data for purposes of conducting evaluations and assessments of PSAP personnel performance, i.e. quality assurance and quality monitoring activities.
- EE. The Logging function shall support Retrieval of Logged Data for purposes of producing external copies. Examples would be copies produced in response to a subpoena, request from a Prosecutor, or media request.
- FF. The Logging function shall support acquisition of Display data (screen capture) via the user interface.
- GG. The Logging function shall support “virtual logger” architecture, i.e. where a Logging function can be shared by multiple agencies, but each agency has access to only its own data and configuration.

- HH. The Logging function shall support fault tolerant data storage such that failure of a single storage medium will not result in loss of data.
- II. The Logging function shall provide and support a fault-tolerant architecture that allows failover to another Logging function in the event the primary Logging Service becomes unavailable.
- JJ. The Logging function shall keep an “audit trail” of all configuration changes and all attempts to access Logged Data (successful and unsuccessful). This audit trail shall contain the type of access or change the parameter or data accessed the username, and the date/time of the access or change. The audit trail data constitutes a “chain of custody” record for the referenced data or configuration parameters.
- KK. The Logging function shall support retention policies for Logged Data that deletes expired data as required by local policy rules. These retention policies must be capable of operating in the “virtual logger” architecture described above.
- LL. The Logging function shall support “functionality that allows the user to mark certain Logged Data to NOT be deleted when its retention period has expired.
- MM. The Logging function shall support time synchronization.

7 Location and Routing Database Management

7.1 Call Data Error Correction

(Submit caller information error report to the originating data provider for correction.)

- A. The system shall provide the capability to document incorrect call information and any associated data received as part of call treatment.
- B. The system shall pre-populate the discrepancy report with the associated source data,
- C. The system shall provide the capability for the user to submit a discrepancy report for correction.
- D. The system shall determine the entity(s) responsible for correcting the source data.
- E. The system shall transmit the discrepancy report to the entity(s) responsible for correcting the source data.
- F. The system shall pre-populate the location discrepancy report with call identification information.
- G. The system shall pre-populate the location discrepancy report with the incorrect information.
- H. The system shall provide the capability for free form text in discrepancy and status reports.

- I. The system shall provide the capability for the entity(s) responsible for correcting the information to return an incident identifier for the discrepancy to the initiating agency.
- J. The system shall provide the capability for the entity(s) responsible for correcting the information to provide a completion status report to the initiating agency.
- K. The system shall provide an automated process for the requestor to determine the status of an outstanding request.

7.2 Location Validation

(Receive and electronically validate location-originating caller location information (civic or geospatial).)

- A. The system shall recognize Call Location Information formatted to NENA Approved Standard Formats & Protocols (e.g. PIDF-LO).
- B. The system shall check Call Location for unrecognizable data type.
- C. The system shall perform location validation on civic addresses.
- D. The system shall check Call Location for garbled data.
- E. The system shall check Call Location fields for logical data ranges.
- F. The system shall check Call Location fields for logical content.
- G. The system shall make use of Default routing in the event of a failed location determination attempt.
- H. System shall support the ability to provide and filter updates to the location information.
- I. The solution shall specify when multiple locations are permitted, what the interpretation of multiple locations shall be, and what the functional elements must do with the locations.
- J. The system shall permit location and address validation by any entity capable of routing an emergency call.

8 Recommended Reading and References

The following documents were used in the preparation of this standard:

- United States Department of Transportation System Description and Requirements Document
- US Department of Transportation Next Generation 9-1-1 (NG9-1-1) System Initiative System Description and Requirements Document

http://www.its.dot.gov/ng911/pdf/NG911_HI_RES_Requirements_v2_20071010.pdf

9 Exhibits

None

10 Previous Acknowledgments

None

NENA

Security for Next-Generation 9-1-1

Standard

(NG-SEC)



NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
NENA 75-001, Version 1, February 6, 2010

Prepared by:

The National Emergency Number Association's (NENA) Security for NG9-1-1 Working Group; a joint working group of the CPE Committee and the Next Generation Integration (NGI) Committee.

Published by NENA
Printed in USA

NENA STANDARD DOCUMENT

NOTICE

The National Emergency Number Association (**NENA**) publishes this document as a guide for the designers and manufacturers of systems to utilize for the purpose of processing emergency calls. It is not intended to provide complete design specifications or to assure the quality of performance of such equipment.

NENA reserves the right to revise this NENA Standard for any reason including, but not limited to:

- conformity with criteria or standards promulgated by various agencies
- utilization of advances in the state of the technical arts
- Or to reflect changes in the design of equipment or services described herein.

It is possible that certain advances in technology will precede these revisions. Therefore, this NENA Standard should not be the only source of information used. **NENA** recommends that readers contact their Telecommunications Carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone companies, etc.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
4350 N Fairfax Dr, Suite 750
Arlington, VA 22203-1695
800-332-3911
or: nrs-admin@nena.org

Acknowledgments:

The National Emergency Number Association (NENA) Joint CPE Committee and Next Generation Integration (NGI) Committee developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

Version [1], Approval Date, [02/06/2010]

Members	Company
Smith - CISSP, Jeremy, WG Co-Leader	L R Kimball
Vanauken-ENP, Gordon, WG Co-Leader	L R Kimball
Allocco, Jim	Spectracom Corporation
Armstrong, Mike	Verizon
Boyken, Bill	AT&T
Corprew, Charles	AT&T
Dantu, Ram	
Davis, Kenneth	Sangamon County ETSD
Dilday, Clay	North Central Texas Council of Govt.
Erdman, Bob	Amcom Software
Frye, Richard T	FRYE-COMM Consulting LLC
Good, Travis	Center for Infrastructure Assurance and Security
Harry, William	
Hayes, David W	L R Kimball
Humrich, Timothy	Qwest
Irons, Johnny	9-1-1 ACOG
Irwin, Dave	Washington Military Department, Emergency Management Division
Jones-ENP, Rick	NENA
Kaczmarczyk, Casimer M	Verizon
Kleck, Kevin	Tarrant County 9-1-1 District
Kleckner, Lori	State of Missouri
Lag Reid, Steve	King County, E9-1-1 Program.
Lewis, Shelby	Positron
Lipinski, Jim	State of Vermont
Maroney, Craig	EMC LLC
Mathis, CISSP ENP PSNP, Ron	Intrado Inc.
McClure, ENP, Nate	CTA Communications
McIntire, Clay	North Central Texas Council of Governments

Moody, Martin D	Metro Emergency Services Board
Oenning, Bob	State of Washington
Ogletree, Brett	
Payne, Mark	Denco Area 9-1-1 District
Porter, RD	State of Missouri
Range, Bill	Dept of Finance and Administration, State of New Mexico
Rosen, Brian	NeuStar
Schlesinger, Jerry	RCC Consultants, Inc.
Seet, Susan M	Texas Commission on State Emergency Communications (CSEC)
Skain, John	Clinton County 9-1-1
Slivka, Joe Ben	Summit County Communications Center
Stork, ENP, Maureen	
Sylvester, Robert L.	Convergent Technologies, Inc.
Thakur, Vikram	
Tschofenig, Hannes	Nokia Siemens Networks
Vick, Chuck	Verizon Business
Vislocky, Mike	Network Orange, Inc.
Walthall, CISSP, Robert	AT&T
Whitehurst, William Ron	Cbeyond Communications
Wilcox, Nathan G	microDATA
Williams, Dwayne	CIAS
Winegarden, Jim	Qwest Communications
Wise, Marc	AT&T

This working group would also thank Tom Breen, Technical Committee Chair/Liaison; Tony Busam, Technical Committee Vice-Chair/Liaison; Pete Eggimann, Operations Committee Chair/Liaison; Wendy Lively, Operations Committee Chair/Liaison; Roger Hixson, Technical Issues Director; and Rick Jones, Operations Issues Director for their support and assistance. Additionally, the working group would also like to give a special thank you to Barbara Thornburg whose assistance in formatting was exceedingly helpful.

TABLE OF CONTENTS

1 EXECUTIVE OVERVIEW7

2 INTRODUCTION.....7

2.1 OPERATIONAL IMPACTS SUMMARY7

2.2 SECURITY IMPACTS SUMMARY7

2.3 DOCUMENT TERMINOLOGY7

2.4 REASON FOR ISSUE/REISSUE.....8

2.5 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK8

2.6 DATE COMPLIANCE8

2.7 ANTICIPATED TIMELINE.....8

2.8 COSTS FACTORS8

2.9 FUTURE PATH PLAN CRITERIA FOR TECHNICAL EVOLUTION8

2.10 COST RECOVERY CONSIDERATIONS.....9

2.11 ADDITIONAL IMPACTS (NON COST RELATED)9

2.12 INTELLECTUAL PROPERTY RIGHTS POLICY9

2.13 ACRONYMS/ABBREVIATIONS9

3 TECHNICAL DESCRIPTION.....10

3.1 SEVERITY CATEGORIES.....10

3.2 STATEMENT OF COMPLIANCE10

3.3 ROLES & RESPONSIBILITIES10

4 SECURITY POLICIES11

4.1 SENIOR MANAGEMENT STATEMENT OF POLICY11

4.2 FUNCTIONAL POLICIES.....12

4.3 PROCEDURES12

5 INFORMATION CLASSIFICATION AND PROTECTION12

5.1 OVERVIEW12

5.2 ROLES AND RESPONSIBILITIES IN INFORMATION CLASSIFICATION AND PROTECTION13

5.3 INFORMATION CLASSIFICATION GUIDELINES.....14

5.4 PROTECTING SENSITIVE INFORMATION.....14

5.5 DEFAULT CLASSIFICATION18

5.6 AUTHORIZING ACCESS TO INFORMATION18

5.7 SAFEGUARDING ELECTRONIC INFORMATION19

5.8 TRANSPORT AND SHIPPING OF ELECTRONIC MEDIA AND DEVICES19

5.9 SAFEGUARDING PRINTED INFORMATION/MATERIAL20

5.10 SENSITIVE INFORMATION DESTRUCTION & SANITIZATION22

6 GENERAL SECURITY22

6.1 GENERAL RESPONSIBILITIES22

6.2 APPLICATION, SYSTEM AND NETWORK ADMINISTRATOR RESPONSIBILITIES.....23

6.3 ENSURING COMPLIANCE FOR RECURRING SECURITY REQUIREMENTS.....23

6.4 NETWORK CONNECTIVITY REQUIREMENTS23

6.5 SECURITY TRAINING.....27

6.6 SUSPICIOUS ACTIVITY27

6.7 GENERAL GUIDELINES FOR DESIGN, DEVELOPMENT, ADMINISTRATION, AND USE OF ANY COMPUTER RESOURCE, NETWORK, SYSTEM OR APPLICATION28



7	SAFEGUARDING INFORMATION ASSETS	28
7.1	IDENTIFICATION AND AUTHENTICATION.....	28
7.2	ACCESS CONTROL.....	34
7.3	CONFIDENTIALITY	41
7.4	INTEGRITY	45
7.5	AVAILABILITY	48
7.6	AUDIT AND ACCOUNTABILITY	50
8	PHYSICAL SECURITY GUIDELINES	51
8.1	BUILDING AND PHYSICAL ACCESS CONTROL	52
8.2	AUTHORIZED PHYSICAL ENTRY	52
8.3	STORAGE MEDIA AND OUTPUT.....	53
8.4	MOBILE DEVICES.....	54
8.5	ENVIRONMENTAL CONTROLS	55
8.6	SERVER ROOM.....	55
8.7	DATA COMMUNICATIONS NETWORKS	57
9	NETWORK AND REMOTE ACCESS SECURITY GUIDELINES	57
9.1	FIREWALLS/SECURITY GATEWAYS.....	57
9.2	REMOTE ACCESS	59
9.3	EXTRANET AND EXTERNAL WAN CONNECTIVITY	60
9.4	INTRUSION DETECTION / PREVENTION.....	61
9.5	LAYER 2 SECURITY AND SEPARATION	62
9.6	NETWORK REDUNDANCY AND DIVERSITY.....	62
10	CHANGE CONTROL AND DOCUMENTATION	63
11	COMPLIANCE AUDITS & REVIEWS	64
12	EXCEPTION APPROVAL AND RISK ACCEPTANCE PROCESS	64
12.1	EXCEPTION APPROVAL AND RISK ACCEPTANCE PROCESS SCOPE.....	65
12.2	ROLES AND RESPONSIBILITIES IN THE EXCEPTION APPROVAL AND RISK ACCEPTANCE PROCESS.....	66
12.3	PROCESS	67
12.4	REVIEW PERIOD	69
12.5	CHANGE OF CIRCUMSTANCE.....	69
12.6	RISK IDENTIFICATION	69
13	INCIDENT RESPONSE & PLANNING	76
13.1	APPENDIX 1: INCIDENT RESPONSE PLANNING.....	77
13.2	APPENDIX 2: PATCHING BEST RESULTS	82
13.3	APPENDIX 3: NG9-1-1 “ENTITY” ARCHITECTURE, DESIGN, ENGINEERING CHANGE CONTROL AND DOCUMENTATION	85
13.4	APPENDIX 4: RISK ACCEPTANCE & APPROVAL FORM.....	88
14	PREVIOUS ACKNOWLEDGMENTS	94



1 Executive Overview

Purpose

The purpose of this document is to establish the minimal guidelines and requirements for the protection of NG9-1-1 assets or elements within a changing business environment.

This document:

- Identifies the basic requirements, standards, procedures, or practices to provide the minimum levels of security applicable to NG9-1-1 Entities.
- Provides a basis for auditing, and assessing levels of security and risk to NG9-1-1 Entities, assets or elements, and exception approval / risk acceptance process in the case of non-compliance to these guidelines.

Scope

This document is applicable to all NG9-1-1 Entities including, but not limited to:

- Public Safety Answering Points
- NG9-1-1 “ESINet”
- NG9-1-1 Service Providers
- NG9-1-1 Vendors
- Any Contracted service that perform functions or services that require securing NG9-1-1 assets.
- Those who use, design, have access to, or are responsible for NG9-1-1 assets (includes computers, networks, information, etc.).

2 Introduction

2.1 Operational Impacts Summary

This document will impact the operations of 9-1-1 systems and PSAPs as standardized security practices are implemented where they have not been in place before. NG9-1-1 Entities will be required to understand, implement and maintain new security solutions, mechanisms and processes.

2.2 Security Impacts Summary

This Security standard may impact other NENA standards and should be reviewed by each committee.

2.3 Document Terminology

The terms "shall", "must" and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words “should,” "desirable" or "preferably".

2.4 Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Version	Approval Date	Reason For Changes
Original		Initial Document

2.5 Recommendation for Additional Development Work

Security is an evolving process and this document should be reviewed on a regular basis for changes.

2.6 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer based or any other type application.

To ensure true compliance, the manufacturer shall upon request, provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945 or equivalent.

2.7 Anticipated Timeline

Applicable sections of this standard should be implemented immediately. NG9-1-1 entities who implement NG9-1-1 components, parts, or solutions must implement all applicable sections of this standard.

2.8 Costs Factors

This standard will have a cost impact to the entities that are impacted. NG9-1-1 Entities are encouraged to expand budgets to specifically include costs related to compliance with this standard.

2.9 Future Path Plan Criteria for Technical Evolution

In present and future applications of all technologies used for 9-1-1 call and data delivery, it is a requirement to maintain the same level or improve on the reliability and service characteristics inherent in present 9-1-1 system design.

New methods or solutions for current and future service needs and options should meet the criteria below. This inherently requires knowledge of current 9-1-1 system design factors and concepts, in order to evaluate new proposed methods or solutions against the Path Plan criteria.

Criteria to meet the Definition/Requirement:

1. Reliability/dependability as governed by NENA's technical standards and other generally accepted base characteristics of E9-1-1 service
2. Service parity for all potential 9-1-1 callers

3. Least complicated system design that results in fewest components to achieve needs (simplicity, maintainable)
4. Maximum probabilities for call and data delivery with least cost approach
5. Documented procedures, practices, and processes to ensure adequate implementation and ongoing maintenance for 9-1-1 systems

This basic technical policy is a guideline to focus technical development work on maintaining fundamental characteristics of E9-1-1 service by anyone providing equipment, software, or services.

2.10 Cost Recovery Considerations

Normal business practices shall be assumed to be the cost recovery mechanism.

2.11 Additional Impacts (non cost related)

Not Applicable.

2.12 Intellectual Property Rights Policy

NENA takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:

National Emergency Number Association
4350 N Fairfax Dr, Suite 750
Arlington, VA 22203-1695
800-332-3911
or: techdoccomments@nena.org

2.13 Acronyms/Abbreviations

Some acronyms/abbreviations used in this document have not yet been included in the master glossary. After initial approval of this document, they will be included. See NENA 00-001 - NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents. Moreover, some acronyms already existing the NENA Master Glossary but shall be updated as noted below. Wikipedia.com was used as a reference for many of these acronyms.

The following Acronyms are used in this document:		
Acronym	Description	** N)ew (U)pdate
(none)		

3 Technical Description

3.1 Severity Categories

Determining whether entities comply with the security requirements stated herein requires an audit to determine compliance. This process is made easier through the definition of severity categories (e.g. High, Medium, or Low) that can be used as a guide for auditors and risk assessors. In this first release of the standard, NENA chose not to include severity categories. It is anticipated that NENA may release a future version of this document that will contain severity categories that would be helpful for auditing and compliance purposes. In the interim, periodic audits are still required as noted later in this document in section 11. NG9-1-1 Entities are required to comply with all applicable portions of the standard.

3.2 Statement of Compliance

Use of the information contained within this document, to develop detailed security requirements, standards, procedures, and practices is recommended for all NG9-1-1 Entity owned infrastructure and devices, in order to provide minimal protection for NG9-1-1 assets and the information and assets of others.

Once detailed security requirements, standards, procedures, and practices are developed by the vendor, non-compliance shall be documented to identify security vulnerabilities, determine associated criticality, and establish a compliance action plan.

Unresolved non-compliance that introduces risk to NG9-1-1 shall require documented risk acceptance as described in Section 12, Exception Approval/Risk Acceptance Process.

3.3 Roles & Responsibilities

An effective security program involves many different roles and responsibilities within, and external to, the NG9-1-1 Entity. Some common roles are listed below (Some roles may be fulfilled by same person).

- **Senior Manager:** Executive or other department manager ultimately responsible for the security of the organization and may be responsible for the operation of all data processing, network, and access to all IT operations of the NG-911 Entity. This person or their designated representative will define security policy as it relates to all systems, networks, and data for the NG9-1-1 Entity as a whole. Many times, this role could be defined and identified by legal statute or regulation.

- **Security Administrator:** Has the functional responsibility for organizational security and is responsible for implementing and administrating security countermeasures in concordance with NG9-1-1 security policies.
- **Data Owner:** Is responsible for appropriately classifying the asset or helping the NG9-1-1 Entity understand its importance in order to establish the necessary level of protection.
- **Data Custodian:** Responsible for ensuring that any security measures required for a particular asset are implemented and maintained.
- **Data User:** The entity that actually uses the data being secured. For example, the Dispatcher is a Data User in that they ‘use’ ALI data to perform their daily tasks.
- **Auditor:** Auditors may be internal or external to the organization and are responsible for examining an organization’s security.

Safeguarding the assets of the organization, both physical and data, is everyone’s responsibility and every individual within the NG9-1-1 Entity should be educated and included in the NG9-1-1 Entity’s security ‘mindset.’

4 Security Policies

The creation of a security policy is the first step in any effective attempt at implementing a security program. A Security Policy is a clearly documented statement of organizational goals and intentions for security, particularly upper management’s commitment to Security. The creation of a security policy requires an organization to recognize, identify, and document its commitment to security. All too often organizations implement security measures without first implementing security policies. This often results in ineffective or unfocused security controls and ultimately leads to more vulnerability. A security policy should facilitate an environment of secure computing and document an organization’s philosophy concerning security.

Security policies vary in size and shape as well as purpose or scope.

At a minimum, an organization shall have the following policies as part of a security program:

- Senior Management Statement of Policy (sometimes called an Organizational Security Policy)
- Functional Policies
- Procedures

4.1 Senior Management Statement of Policy

NG9-1-1 presents new threats and risks. Senior management must be engaged and committed to maintain highly effective security so the rest of the staff can be able to do their part. Security cannot be made someone else’s responsibility; everyone, and especially management, must be involved and vigilant. Creating a senior management statement of policy is crucial to documenting the importance of the computing assets and resources to the organization as well as upper management’s commitment to exercise due care through the definition and management of acceptable operational level standards, procedures, and measures.

The Senior Management Statement of policy shall, at a minimum:

- Identify person responsible for security
- Provide a written description of the security goals and objectives of the NG9-1-1 Entity

4.2 Functional Policies

Functional policies provide a deeper level of granularity after creating an executive management statement of policy. Functional policies must be established prior to the implementation of any actual security measures. Some examples of functional policies include:

- Acceptable Usage Policy (i.e. email, Internet usage, USB storage device, personal computer use, blogging, social networking, etc)
- Authentication/Password policies
- Data Protection Policy
- Wireless Policy
- Physical Security Policy
- Remote access policies
- Hiring practices
- Security enhancements or technology that should be implemented within a NG9-1-1 Entity
- Baseline configurations for workstations existing on the NG9-1-1 Entity network
- Standards for technology selection
- Incident Response Policy

4.3 Procedures

A procedure is the documented method of performing a specific task. As an organization's security policies begin to take shape it will become necessary to document certain tasks such as the procedures on creating new user accounts or the actual steps to allow a vendor access to a server room. Procedures are an important part of any security strategy because they take the guesswork out of certain tasks ensuring consistency and accountability.

5 Information Classification and Protection

5.1 Overview

Information classification is the framework for evaluating and protecting information and assets that contain information owned and used by the NG9-1-1 Entity. Information is categorized based on the sensitivity, applicable policies and/or legal and statutory requirements.

5.2 Roles and Responsibilities in Information Classification and Protection

5.2.1 Data Owner

When a vendor, NG9-1-1 employee, contractor, agent or service provider creates a document, or is designated responsible for a system, device or media containing sensitive information, he/she shall become the data owner of/for it. The data owner responsibilities include:

- Judging the value of the information resource and assigning the proper classification level according to this guideline.
- Periodically reviewing the classification level to determine if the status shall be changed.
- Communicating access and control requirements to the data custodian and users.
- Providing access to those individuals with a demonstrated business need for access.
- Assessing the risk of loss of the information and assuring that adequate safeguards are in place to mitigate the risk to information integrity, confidentiality, and availability.
- Monitoring safeguard requirements to ensure that information is being adequately protected.

5.2.2 Data Custodian

When a vendor, NG9-1-1 Entity employee, contractor, agent or service provider retains Sensitive information, he/she shall become a custodian of that information and is responsible for protecting its confidentiality, integrity and availability according to the rules and regulations established by the originator. At a minimum, the custodian is responsible for:

- Complying with information classification and protection policies on retention and disposal of records and information.
- Providing proper safeguards for the information, including following guidelines in this Guideline for proper disposal. In those cases where information must be printed from electronic media, the custodian must mark the printed information with the appropriate classification.
- Providing proper safeguards for processing equipment, information storage, backup, and recovery.
- Providing a secure processing environment that can adequately protect the integrity, confidentiality, and availability of information.
- Administering access requests to information properly authorized by the originator.
- Using the information only for the purpose intended.
- Maintaining the integrity, confidentiality, and availability of information accessed.

Being granted access to information does not imply or confer authority to grant other users access to that information beyond the normal boundaries established for a given classification. This is true whether the information is electronically held, printed, hardcopy, manually prepared, copied, or transmitted.

5.3 Information Classification Guidelines

Information Classification defines four (4) classifications for information owned or used by the NG9-1-1 Entity as defined later in this document:

- Public
- Sensitive (Internal Use Only)
- Sensitive (Restricted)
- Sensitive (Most Sensitive Information)

NOTE: While other levels or classifications may exist, they may be specific to each organization and therefore, not listed here.

5.4 Protecting Sensitive Information

5.4.1 Classifying Information

NG9-1-1 Entity uses information that it owns as well as information owned by other persons or entities.

NOTE: Information that is proprietary to another company or government agency shall be obtained legally with the agreement of the other company or agency and in compliance with the appropriate code of conduct. Information shall be classified using the highest applicable classification based upon the descriptions below.

Examples of each type of information follow this section and are separated into NG9-1-1 Entity information, and non-NG9-1-1 Entity information (e.g., service provider, third party, and government entities information), and public information.

This section is intended to serve as a guideline to organizations seeking to classify their information. NG9-1-1 entities should ensure they comply with all applicable laws and regulations such as the Freedom of Information Act (FOIA).

The security policy of the NG9-1-1 Entity shall specify which classifications of data it believes are not subject to FOIA.

5.4.2 Public

1. Description
 - a. Information for which there is no value in keeping it secret, or
 - b. Information intended for public disclosure and purposely placed in the public domain, or must be made publicly available per applicable policies, and/or legal and statutory requirements
 1. Does not necessarily imply that the information must be made public
2. Examples of Public Safety Information

- a. Guidance for ordering products and services (i.e. Vendor Product Briefs, RFPs, etc)
 - b. Public directory information (i.e. Phone number to Police Department)
3. Examples of non-Public Safety Information
 - a. Any public domain information (i.e. website addresses, etc)

5.4.3 Sensitive (Internal Use Only)

1. Description
 - a. Information that is sensitive and not intended for public disclosure, whose value could be diminished if publicly disclosed, or
 - b. Information that could be valuable to create unintended obligations or liabilities for Public Safety if revealed outside Public Safety domain, or
 - c. Information that is intended for all employees or authorized contractors or is of such a nature that it is in Public Safety organization's interest to allow any employee to determine if there is a legitimate need to share it with any other employee.
2. Examples of Public Safety Information
 - a. Internal directory entries excluding fields specifically identified in other classification levels,
 - b. General Process and Operational information,
 - c. Service Descriptions,
 - d. Internal communications and instructions,
 - e. Policies, Standards and Guidelines.
 - f. Data relating to Internet usage
3. Examples of non-Public Safety Information
 - a. The same type of information owned by the service provider and third party including government entities.

5.4.4 Sensitive (Restricted)

1. Description
 - a. Information that has a higher level of sensitivity and which the originator determines shall be shared only among specifically identifiable persons or team with a clear need to know, or
 - b. Information that requires a high degree of protection by law and loss or unauthorized disclosure could require notification by Public Safety to government agencies, individuals or law enforcement, or
 - c. Information, that if revealed widely within Public Safety could present an increased risk of compromising computer systems, fraud, or increased probability of disrupting the day to day operation of the Emergency Communication System.
 - d. Not intended for public release

2. Examples of Public Safety Information
 - a. Strategic Operational plans including Fall-Back sites, Fuel Depots, etc.
 - b. Personnel and salary information
 - c. Internal Audit information
 - d. Security information including logs, authentication credentials (passwords and pins), architecture diagrams, and configuration files
 - e. Network information including engineering or architecture diagrams and configuration files related to IT networks
 - f. Research and development information including studies, designs and development plans for new or improved products, services, or processes
 - g. Incident reports and vulnerability
 - h. Attorney-Client Privileged information
 - i. Customer Proprietary Network Information (CPNI) as described in the US Telecommunications Act of 1996
 - j. Firewall rules
 - k. Software source code for critical applications.

3. Examples of non-Public Safety Information
 - a. The same type of information owned by Service Provider or third party including government entities.

5.4.5 Sensitive (Most Sensitive Information)

1. Description
 - a. Information that requires a high degree of protection by law and loss or unauthorized disclosure would require notification by Public Safety to government agencies, individuals or law enforcement, and
 - b. Information that, if made public, could expose NG9-1-1 entities to a risk of physical harm, compromise of undercover operations, public safety operations, fraud or identity theft, etc.

2. Examples of Sensitive (Most Sensitive Information)

The following “Privacy” data elements have been classified as Sensitive (Most Sensitive Information):

Individual Identification	
Data Element	Description
NG9-1-1 Entity User Identification Value	Specific NG9-1-1 Entity UID Value (that are used as a data element, not as a login) shown in association with owner
Drivers License Number	

Nationally-Issued Identification Number	Includes visa and/or passport values
State or Province-Issued Identification Number	
Social Security Number (SSN)	Includes any portion of SSN
Computer Identification and Authentication	
Description	
PINs, Passwords or Passcodes	Values used by a user to allow (authentication of) access to public safety information or service, includes calling card PINs and secret codes
Stored Password Hint Answers	Answers to questions used to retrieve passwords, for example mother's maiden name

Other Data	
Data Element	Description
Date of Birth (DOB)	Includes month, day and year
Biometric Data	Measures of human physical and behavioral characteristics used for authentication purposes, for example voiceprint, retina or iris image, also includes scanned images.
Digitized or Electronic Signatures	A digital representation of a manual signature
56B Background Check Data	Results of background check
Information obtained from NCIC (National Crime Information Center)	NCIC is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, and missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year.
Medical Information	Personal medical information
ALI and ANI information	Phone numbers and addresses

5.4.6 Receipt of Sensitive Information

Sensitive information received from external parties shall be clearly marked by the recipient as sensitive and treated in accordance with any applicable regulations or restrictions (such as those set forth in a contract between NG9-1-1 entities and a Service provider, etc).

The sensitive information of Service Providers or third parties, including government entities, shall, unless otherwise specified in the contract with Service Providers or the third party, be safeguarded in the same manner as NG9-1-1 Entity information of like sensitivity or pursuant to Nondisclosure Agreements in place which may govern handling of such data or local, state or federal laws governing sensitive data.

5.5 Default Classification

If the classification of information is unknown, the information shall be treated as Sensitive (Internal Use Only) until the proper classification is determined or it is determined to be Public Information by the originator or other applicable laws and regulations.

5.6 Authorizing Access to Information

All access to information by any service provider, vendor, NG9-1-1 Entity employee or contractor shall comply with applicable codes of conduct, policies, contracts, laws and regulations. Persons not authorized to view or modify information shall be prohibited from viewing or modifying information.

Persons who are not NG9-1-1 Entity employees (e.g., contractors, suppliers, or vendors) shall have appropriate contractual agreements in place that establish their relationship to the NG9-1-1 Entity and authorize their access to NG9-1-1 Entity resources prior to being granted access to information of any classification other than Public.

5.6.1 Public

Public information may be shared with anyone inside or outside the service provider, vendor, or NG9-1-1 Entity and may be presented or published in the public domain.

5.6.2 Sensitive (Internal Use Only)

Internal Use Only information may be shared with any employee with a legitimate need, and may be shared with any non-payroll worker (e.g., contractor) who is authorized.

Release of Sensitive (Internal Use Only) information shall be documented when released subject to an FOIA request.

5.6.3 Sensitive (Restricted)

Restricted information shall be shared only with the explicit permission of the originator. Permission shall be in writing. Electronic communication is acceptable. Electronic systems that support the notion of role-based approval or rights based responsibilities are allowable.

Release of Sensitive (Restricted) information shall be documented when released subject to a FOIA request.

5.6.4 Sensitive (Most Sensitive Information)

Most Sensitive Information shall only be shared or modified with the explicit permission of the originator and/or in accordance with applicable laws and regulations. Electronic systems that support the notion of role-based approval or rights based responsibilities are allowable.

Release of Sensitive (Most Sensitive) information shall be documented when released subject to an FOIA request.

5.7 Safeguarding Electronic Information

Where **Sensitive (Most Sensitive Information)** data is allowed to be stored or transmitted on a network between devices, whether inside or outside the NG9-1-1 Entity it must be encrypted. In NG9-1-1 systems, the encryption algorithm shall be AES.

Where Sensitive (Internal Use Only), Sensitive (Restricted), and Sensitive (Most Sensitive Information) data stored on removable or portable media (such as USB flash drives, thumb drives, memory sticks, external hard drives, or CDs), and mobile computing devices (such as laptops, PDAs or blackberries), it:

Shall either be kept in the direct supervision of the custodian or physically secured from unauthorized access (e.g., in a locked office, desk, or filing cabinet), and

Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., shall not be placed in taxi trunk/boot, bus hold/baggage storage, checked-in on airplane).

However, mobile computing devices containing Sensitive (Most Sensitive Information) shall not be taken outside NG9-1-1 Entity controlled space, but if there is an overriding business need to do so then approval shall be documented in policies that allow applicable roles to have such rights. Exceptions to the policy shall be documented in writing.

Whenever systems containing vendor, service provider or NG9-1-1 Entity information requires repair, the service provider or vendor employees and contractors shall use only approved repair processes, groups or locations and in accordance with applicable non-disclosure agreements, laws, regulations and policies to ensure that information contained on the devices is safeguarded in keeping with its sensitivity level.

5.8 Transport and Shipping of Electronic Media and Devices

Media or devices containing Sensitive (Most Sensitive Information) **shall** be hand delivered by the custodian. However, if there is an overriding business need to do otherwise then approval **shall** be obtained from a senior Manager and be shipped in sealed packages utilizing recorded/certified delivery.

Media or devices containing sensitive information, other than Sensitive (Most Sensitive Information), shall be shipped in sealed packages either via interdepartmental mail or utilizing recorded/certified delivery via a mail delivery service.

5.9 Safeguarding Printed Information/Material

5.9.1 Sensitive (Internal Use Only) – Printed Material

1. Inside Controlled Space:
 - a. Shall be kept away from visitors who have no need to see the information
 - b. No Controls required when distributed within the controlled space
 - c. Shall supervise sending and receiving fax machines with authorized personnel, or use fax machines in offices/areas where access is limited to authorized personnel.
 - d. Shall be shredded after use
2. Outside Controlled Space:
 - a. Shall be secured from unauthorized access
 - b. Shall be kept in the direct supervision of the custodian
 - c. Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage)
 - d. Shall supervise the printer or copier with an authorized person for the information
 - e. Shall use a sealed envelope whenever delivery is to a location external to the controlled space or whenever the delivery utilizes non-company personnel or service.
 - f. Shall supervise fax machines that are located outside the controlled space with authorized personnel.
 - g. Shall be shredded after use

5.9.2 Sensitive (Restricted) – Printed Material

1. Inside the Controlled Space:
 - a. Shall be kept away from casual observers.
 - b. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe).
 - c. If the controlled space is only accessible to the designated "Team", it is not necessary to keep hidden or physically secured when unattended.
 - d. Shall either supervise the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.
 - e. Shall be hand delivered by originator or custodian.
 - f. Shall use double envelopes with the inner envelope marked "Private" when using internal mail.
 - g. Shall supervise sending and receiving fax machines with authorized personnel, or use fax machines in offices/areas where access is limited to authorized personnel.
 - h. Shall use special bins provided or be shredded

2. Outside the Controlled Space:
 - a. Shall be kept away from casual observers.
 - b. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
 - c. Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., taxi trunk/boot, bus hold/baggage storage, checked baggage on airplane).
 - d. Shall supervise the printer or copier with a person authorized for the information.
 - e. Shall use double envelopes with the inner envelope marked "Private" and send recorded/certified delivery whenever delivery is to a location external to controlled space or whenever the delivery utilizes non-company personnel or service.
 - f. Shall supervise fax machines that are located outside NG9-1-1 Entity controlled space with authorized personnel.
 - g. Shall be shredded

5.9.3 Sensitive (Most Sensitive Information) – Printed Material

1. Inside the Controlled Space:
 - a. Shall be kept away from casual observers.
 - b. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe).
 - c. Shall either supervise the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.
 - d. Shall be hand delivered by the originator or custodian.
 - e. Shall not be faxed.
 - f. Shall be shredded.
2. Outside the Controlled Space:
 - a. Shall never be taken outside the controlled space.
 - b. If there is an overriding business need then:
 1. Shall obtain approval from a Senior Manager.
 2. Shall be kept away from casual observers.
 3. Shall be kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
 4. Shall not leave the direct supervision of the custodian when traveling on public transport (e.g., taxi trunk/boot, bus hold/baggage storage, checked baggage on airplane).
 5. Shall not print/copy outside the controlled space. Or shall supervise the printer or copier with a person authorized for the information.
 6. Shall hand deliver by the data owner or data custodian.
 7. Shall not be faxed.
 8. Shall be shredded.

5.10 Sensitive Information Destruction & Sanitization

5.10.1 Hard Copies or Printed Material

When hard copy Sensitive documents are no longer needed or required to be retained, they shall be properly disposed.

Some locations will have special locked "sensitive material" bins (which prevent access to documents once inserted) where documents may be left. These bins shall be periodically emptied and the contents taken away for secure shredding.

Where "sensitive material" disposal bins are not available, shredding shall be performed. Shredding shall be done in such a way that it is impractical to reconstruct either the whole document, or a large enough part, from the pieces such that the information contained on it might be compromised. The recommended approaches being to either use cross-cutting into pieces/confetti (width (max): 3/4 inch or less and length (max): 2.5 inches or less) or continuous cutting/shredding into strips (width max: 5/8 inch or less and length: indefinite or less).

5.10.2 Sanitizing Media or devices whose media contains Sensitive data, e.g., PCs, CDs, Hard disks, Tapes, USB drives

All media types shall have Sensitive information sanitized (rendered irretrievable), in a manner that will prevent misuse or unauthorized disclosure prior to repair, reuse or disposal. It is well known that even after data has been deleted or moved the data may actually still reside on the device. This is because many operating systems do not actually erase the data, but only remove the pointers between the directory and the data locations. This may result in the data being accessible by unauthorized person(s) using readily available utility programs.

Examples of media sanitization approaches include:

- Degaussing
- Magnetic Media Erasing
- Disintegrators
- Optical Media Destruction
- Disk Erasers
- Services that offer media destruction

6 General Security

6.1 General Responsibilities

Agreements between the NG9-1-1 Entity and vendors, contractors or suppliers for the purchase, development, or support of information resources or services shall incorporate the appropriate

contractual security requirements, detailed roles and responsibilities (including Application, System and Network Administrators) and applicable security review or assessment to ensure the protection of all relevant information, systems, and services. “Information resources” shall include any owned or managed systems, applications, and network elements, and the information stored, transmitted, or processed with these resources.

Contractors, suppliers and supplier’s employees and subcontractors shall protect information resources in accordance with the terms and conditions of applicable contractual agreements between the contractor or supplier and NG9-1-1 Entity.

In addition, it shall be the responsibility of all contractors, suppliers and supplier’s employees and subcontractors to comply with applicable federal, state, and local acts, statutes, and regulations that relate to the control and authorized use of information and information resources.

These requirements apply to the entire supplier or supplier subcontractor environment that may impact the information resources used to support the contract.

6.2 Application, System and Network Administrator Responsibilities

Application, system, and network administrators shall perform self-review on the systems for which they have operational responsibility at least once a year to ensure that the systems are compliant with all security requirements. These assessments shall be in writing and communicated to the designated security manager and NG9-1-1 Entity management. Entities may choose to outsource the self-review activity to designated IT security firms as noted in section 11 of this document.

A copy of current security self-reviews or security assessments/audit reports shall be retained for future reference and audit purposes until superseded by another security assessment or until the system is retired.

6.3 Ensuring Compliance for Recurring Security Requirements

The applicable Application, System and Network Administrator shall identify which security solutions have or require periodic review. For example: Intrusion Prevention Systems, Event Logs.

The applicable Application, System and Network Administrator shall implement and execute a plan to periodically review items identified in preceding section and take appropriate action.

6.4 Network Connectivity Requirements

6.4.1 General

Network security forms a cornerstone of the overall security posture for any NG9-1-1 Entity and connecting entities. An improperly secured network can present many problems to an NG9-1-1 Entity such as providing an avenue for intrusion by unauthorized machines or personnel, loss of service including an inability to accept critical calls from the public or a conduit for propagation of malicious or destructive code. While no network can be declared totally secure, there are

measures that can be taken to significantly improve the overall security of a given network. The next few sections will provide requirements for improving network security.

6.4.2 Purpose

When architecting networks it is useful to clearly define a purpose or mission for any given network so that the appropriate security measures can be implemented

6.4.3 Inventory

An accurate and current inventory is a key requirement for network security. Such an inventory will provide a basis for comparison to detect unauthorized devices which may appear on the network. All devices in the inventory shall comply with other aspects of this and other relevant guidelines. Various tools exist which can assist with the creation of an accurate inventory and provide an assessment of the security compliance of various platforms on the network. Inventories shall be classified appropriately and in accordance with the implemented information classification and protection policy.

6.4.4 Controlling Points of Access

All administrative access to any network shall be precisely controlled with appropriate identification, authentication and logging capabilities. All points of ingress and egress to a network shall be fully documented, approved and protected. Such points may include but are not limited to the following: modems, dual-homed platforms, wireless routers or access points, routers and firewalls or gateways. Even different network technologies shall be clearly documented such as those used for "out of band" access, typically for operations access. Points of access that do not support the objectives of the call center shall be eliminated. Remaining points of entry shall be controlled. Many technologies exist for this purpose including firewalls, intrusion detection and prevention devices, proxies, etc. In no case shall any uncontrolled point of entry or "gateway" be permitted on a network.

For standards relating to Remote Access see section 9.

6.4.5 Use of Dual or Multi-Homed Device

A dual or multihomed computer is a host (this does not refer to routers, firewalls, switches, etc, in this context) connected to two or more networks or having two or more network addresses. For example, a call taking computer may have a network interface connected to a CPE network and another connected to a CAD network.

Multihoming computers for vendor convenience and isolating problems introduces security risks and creates avenues for malicious code to more easily spread amongst the networks as well as making the network configuration more complex. Therefore, multihomed computers should be avoided. Instead, if business requirements dictate that a computer must access resources resident on different networks, the networks should be connected together and the appropriate security countermeasures, including those described in this document, should be implemented.

When multihoming computers cannot be avoided, the following guidelines are provided:

- Connecting multihomed computers to networks that have differing security postures shall not be allowed. For example, one network utilizes antivirus software while the other network does not.
- Operating Systems should be hardened
- Application should be hardened
- Anti-virus running on both networks and on multihomed computer
- Host Intrusion Prevention Software (IPS) running on multihomed computer
- IP-forwarding explicitly disabled
- Other appropriate security countermeasures, including those described in this document should be implemented

Important Note: The preceding sections do not apply to, affect or eliminate the need or capability for a computer to utilize more than one network interface card connected to the *same* network for redundancy purposes (i.e. Network Interface Card Teaming for bandwidth aggregation, failover, and/or isolated tape backup or management network specifically for system administration purposes).

6.4.6 Wireless access

Wireless networks do not utilize cable media (ex. Ethernet, COAX) to transmit signals for carrying data. Typically, wireless networks utilize radiated power or radio signals of various formats. Since these signals are not confined to a physical space such as building walls, security measures must be taken to manage risks associated with wireless media. The following sections will list common types of wireless network technologies and provide requirements and recommendations for securing them.

6.4.6.1 802.11 LANS – (802.11 a.b.g.n.)

Wireless Local Area Networks, hereafter referred to as 802.11 LANs, are networks that allow for LANs to be deployed using wireless technologies such as 802.11g, 802.11b, etc. 802.11 LANS shall not be deployed without the following security measures in place under any circumstances. 802.11 LANS shall implement the following at a minimum:

- Default router management password shall be changed and treated as administrator level passwords for syntax, history and periodic changes
- Router management over the wireless link shall be disabled. Router management shall use an encrypted protocol (ex https) whenever available.
- Service Set Identifiers (SSID) shall be changed from default value to an identifier not easily associated with the NG9-1-1 Entity or otherwise easily guessed.
- SSID broadcast shall be disabled
- Wireless security (encryption) shall be enabled. Wired Equivalent Privacy (WEP) shall not be used. 802.11 Protected Access (WPA) or greater (WPA2 with AES and Temporal Key Interchange Protocol (TKIP) 802.11i) is required.

- TKIP passphrase shall be non-trivial and meet minimum length and complexity requirements defined in this document for passphrases.
- Rekey interval shall be 3600 second maximum.
- The 802.11 LAN shall be dedicated to the NG9-1-1 Entity and not shared with any other user community (such as public LANS).
- Media Access Control (MAC) address filtering shall be enabled and the MAC filter list shall be reviewed and purged at a minimum of monthly and immediately whenever a machine is retired from the network. .

Ad hoc modes shall be disabled.

802.11 LANS should consider the following additional measures to minimize risks.

- Maximum encryption key lengths supported by the device should be utilized
- Router Dynamic Host Configuration Protocol (DHCP) services should be disabled and require static Internet Protocol (IP) Addresses for connected devices. If DHCP must be used, the DHCP scope (range of addresses) should be kept to a minimum length.
- If DHCP is used, automatic assignment of other services (e.g. DNS servers, WINS servers) is allowed and should be reviewed in concert with the overall security plan.
- The default SSID channel should be changed from its default value.
- The 802.11 LAN hardware should utilize a third party authentication service for management (such as TACACS, Radius) when supported.
- The 802.11 LAN should utilize a Network Access Control (NAC) technology to ensure proper patching and malicious software screening is performed on all LAN assets. At a minimum, use of a rogue device detection capability is **STRONGLY** recommended. Also, use of Intrusion Detection Systems (IDS) is encouraged on 802.11 LANs.
- The 802.11 LAN should be separated from other networks by a firewall which limits access to and from the wireless network on an exception basis only.
- Users should be authenticated to the wireless LAN using a two factor mechanism or emerging authentication standards like 802.1x.

6.4.6.2 Bluetooth Networks and similar short range device-specific proprietary wireless networking solutions

Bluetooth is an open wireless protocol for exchanging data over short distances from fixed and mobile devices thus creating personal area networks (PANs).

- Bluetooth wireless networking should be avoided where possible, including wireless headsets and other human interface devices such as mice and keyboards.
- Bluetooth shall not be used for “backups” for any medium or device which contains sensitive (internal data only) or greater data.
- Bluetooth, if used, must be configured to require device identifiers.
- Presence of frequency hopping, phase shifting, device serialization or other such technologies alone shall not satisfy encryption or identification requirements.

6.4.6.3 Broadband Wireless Connections

In 2002 the FCC designated 50 MHz of spectrum in the 4940-4990 MHz band for use in support of public safety. A license from the FCC must be obtained in order to utilize the 4.9 GHz band.

The FCC has approved any terrestrial based radio transmission including data, voice, and video - including Point-to-Point and Multipoint operations for use in this spectrum. Current deployments include: Wireless LANs for incident scene management, Mobile data, Video security, VoIP, PDA connectivity, Hotspots, and T1 line replacement or redundant WAN links.

The requirements and guidelines specified in NG-SEC apply to all communications in the 4.9G MHz band. All communications over this band should be encrypted. Authentication, authorization, and accountability should be maintained. Firewalls shall be deployed at network boundaries.

6.4.6.4 Broadband wireless technologies for mobile users (e.g. Laptop, handheld and other devices)

1. Each of these technologies (I.e. 3G, EDGE, etc) should be regarded as a “remote access” capability and all security standards relevant to remote access found in this document are applicable.

6.5 Security Training

NENA recognizes that security awareness training is critical to any organization’s security strategy and security operations. People are in many cases the last line of defense against many threats such as malicious code, disgruntled employees, and malicious third parties. Therefore, people need to be educated on what the organization considers appropriate security-conscious behavior, the applicable security policies implemented at their organization and what security best practices they need to incorporate in their daily business activities. All Public Safety employees shall annually complete security awareness training as established by each Public Safety Organization.

Additionally, entities responsible for system and security administration (including those contracted to do such tasks) shall employ individuals who have received current security training on their assigned system(s). It is the right of the 9-1-1 Call Center or similar agency to specify that a contracted agency hold specific or certain certifications to prove compliance with this requirement.

6.6 Suspicious Activity

Any suspicious or unusual activity, which may indicate an attempt to breach the integrity of Public Safety’s networks and systems, shall be reported immediately to an established Security Point of Contact / Team or equivalent. Any, and all, actual, attempted, and/or suspected misuse of Public Safety assets shall be reported immediately to the appropriate organizations.

6.7 General guidelines for design, development, administration, and use of any computer resource, network, system or application

Design, development, administration, and use of any computer resource, network, system, or application should always enable compliance with all security policy and requirements applicable to its intended use. Incorporating security into new products, services, systems, and networks before they are deployed shall be a priority. Security policy and requirements, and/or risk assessments should be a consideration in any development or product realization process. A security assessment of the controls and procedures should be conducted and documented before deployment to certify the compliance with security policy. This document should be retained as evidence for any future audit.

7 Safeguarding Information Assets

7.1 Identification and Authentication

Identification is the process by which one entity recognizes another entity, e.g., user, system or process.

Authentication is the provision of assurance of the claimed identity of an entity (e.g., individual user, machine, software component, etc.) The result may be Pass or Fail. The level of certainty with which the entity can be linked to the claimed identity will vary according to the authentication method used and operating practices.

In electronic information systems, authentication systems are hardware, software, or procedural mechanisms that enable a user to obtain access to network and / or computing resources.

Typically, a user identifies him or herself to the system by entering a unique User ID and password in response to a prompt. However, the authentication credential may take several forms, including passwords, digital certificates, or other shared-secret information (a combination of a token or smartcard used with a Personal Identification Number (PIN), also known as a Personal Identifier (PID)).

7.1.1 Unique Identification and Authentication

All computer resources, systems, applications, and networks, which process Public Safety data, or data of others that Public Safety is obligated to protect, shall positively and uniquely identify and authenticate individual users prior to granting access. Any credentials used to identify and authenticate users or systems accessing computing or networking resources shall be assigned to individuals and not shared with anyone else, including work associates and managers.

7.1.2 User Access Management

The administration of user or entity access and accounts is a major component of security administration. The following outlines the minimum guidelines for processes such as assigning new entity accounts, resetting passwords, establishing resource access, and removing inactive accounts.

Requests for establishment of new entity accounts, User IDs and file and resource authorization shall be made through a process that can be documented and audited.

The request shall be approved by the authorized representative of the agency.

Personnel performing entity or security administration functions shall be responsible for ensuring that only approved entities are granted use and access to Public Safety's information resources. This requires that the identity of the requestor and of the approver, if required, be validated. This includes requests for password/PIN resets.

7.1.2.1 Changing Access

When a user changes job assignment, including promotion, demotion or termination:

1. The user's manager shall review the users access needs and notify all responsible administrators/help desks of job assignment changes within 24 hours.
2. Administrators or help desks shall delete or disable the IDs, or modify command and data access permissions of users within 24 hours of notification. Where access is no longer required the User ID shall be disabled and ultimately deleted when all use of the account is complete.

7.1.2.2 Disabling or Deleting Access

User IDs that have had no activity for 90 days should be reviewed with the approving manager for possible removal or deactivation. If the manager confirms that it is no longer required the User ID shall be deleted, otherwise it should be disabled. If feasible, system administration personnel should be informed of the need to remove an Entity's access to Public Safety information resources as far in advance of the need to remove the access as possible.

7.1.3 System to System Access

System to system access shall never mask individual accountability for transactions.

In any method of system to system data transfer, the source system shall first be authenticated before each transfer session. In the case of push technology, the destination shall be authenticated by the source. If the transfer method uses a continuous connection, authentication shall be performed at the initial connection.

Each system, application and machine shall have an identification and authentication mechanism built into the access path. One system/application/machine may perform security functions and controls for another system/application/machine dependent on the security relationship of the entities. The security services relationship shall be documented and approved in writing by the management of the interfacing systems/applications/services, and shall include a description of the security functions one entity is responsible for performing for the other.

7.1.4 Unsuccessful Login Attempts

A failed login attempt shall not identify the reason for the failure to the user, only that the login was incorrect, so as not to aid in subsequent unauthorized attempts to guess the right combination.

System login procedures shall be designed and implemented with a mechanism that will prevent the use of repeated login attempts to guess or otherwise determine a valid login identification and authentication combination. Systems shall lock the user out after no more than 5 failed login attempts.

7.1.5 Default Credentials and Control of Authentication Credentials

Null and factory default credentials shall be changed whenever installing new equipment or software. This includes all operating systems, applications and network infrastructure devices.

Authentication credentials shall not be visibly displayed when entered on computer screens, and when stored on computers, they shall be encrypted. When in written form, they shall be kept under lock and key and kept separated from associated User IDs and/or application names or devices.

Where two-factor authentication is used, e.g., SecurID + PIN, or Certificate + Passphrase, the two authentication factors shall not be stored in such a manner that a single event could compromise both factors.

Temporary credentials (which are credentials that are assigned by the Administrator, either when the account is initially created, or subsequently when a reset or reactivation is required) associated with User IDs shall require the user to change them at the first login. Where the technology permits temporary credentials shall be disabled if not changed within 30 days. If a credential does become, or is suspected of being, compromised, it shall be changed immediately.

7.1.5.1 Passwords

User Accounts and Passwords are common and effective mechanisms to control access to systems. It is important to not only require that all accounts used to access systems have passwords but that the passwords follow specific guidelines to maximize their success.

1. All User Accounts shall require a password
2. Password shall be adhere to the requirements listed in Table below:

Password Requirements

Option	Explanation	Required Minimum Value
Passwords must meet complexity requirements	Passwords are not based on the user's account name. Contains characters from three of the following four categories: <ul style="list-style-type: none"> • Uppercase alphabet characters (A–Z) • Lowercase alphabet characters (a–z) • Arabic numerals (0–9) • Non-alphanumeric characters (for example, ! \$#,%) 	Enabled
Minimum password length	The setting determines the minimum number of characters that a user's password must contain. It is recommended that you change this setting from the default value of 0.	8
Minimum password age	This setting determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again. A value of a few days discourages rapid password recycling while still permitting users to change their own passwords if desired. Note that setting this parameter to a value higher than the maximum password age forces users to call the IT department to change their passwords, which increases costs to the organization	3
Maximum password age	This setting determines the period of time (in days) that a password can be used before the system requires the user to change it. The best defense against impersonation is to require that users change their passwords regularly. This reduces the amount of time available for attackers to crack unknown passwords, and it periodically invalidates any password that has been stolen by other means.	60 (30 is recommended)

Enforce password history	This setting determines the number of unique new passwords that have to be associated with a user account before an old password can be re-used. It also rejects new passwords that are too similar to previous passwords. This feature prevents users from circumventing password lifetime restrictions by reusing their old password. The default value is 1. Most IT departments choose a value greater than 10.	10
--------------------------	---	----

3. Where feasible, authentication schemes shall provide for password exchange in a format that cannot be captured and reused/replayed by unauthorized users to gain authenticated access, e.g., random password generating tokens or one-way encryption (also known as hashing) algorithms.
4. Passwords should not be hard coded into automatic login sequences, scripts, source code and batch files, etc, unless required by business need and then only if protected by security software and/or physical locks on the workstation, and passwords are encrypted.
5. Temporary passwords may be used when creating new accounts or resetting passwords, however, temporary passwords shall be required to be changed upon initial login.

The following additional password **guidelines** are provided to assist in educating users on how to create passwords:

- Password construction should be complex enough to avoid use of passwords that are easily guessed, or otherwise left vulnerable to cracking or attack. Names, dictionary words, or combinations of words shall not be used; nor shall they contain substitutions of numbers for letters, e.g., s3cur1ty. Repeating numbers or sequential numbers shall also not be used
- Passwords should not contain sequences of three (3) or more characters from the user's login ID or the system name.
- Passwords should not contain sequences of three (3) or more characters from previous chosen or given passwords.
- Passwords should not contain a sequence of two (2) or more characters more than once, e.g., a12x12.
- Passwords used to access Public Safety systems and resources should not be used on any external systems, e.g., Home PC's, Internet sites, shared public systems.

7.1.5.2 Passphrases

Passphrases are generally more secure than traditional passwords and should be used whenever possible. A Passphrase is simply a sequence of words or phrases used in place of a traditional password” to access a system.

Passphrases, when used, shall comply with the following minimum requirements:

1. Should be at least fifteen (15) characters in length.
2. Shall not use repeating words, or sequential characters or numbers.
3. Alpha, numeric and special characters may all be used.
4. Passphrases are case sensitive.

Where automatically set or set by administrator, the initial passphrase shall be randomly generated and securely distributed. First-time users may create their own passphrase after authenticating.

Users shall have the capability of changing their own passphrase online. The old passphrase shall be correctly entered before a change is allowed. A lost or forgotten passphrase can be reset only after verifying the identity of the user (or process owner) requesting a reset.

For a general System User, passphrases shall automatically expire every 180 days or less. Systems shall notify users at expiration time and allow the user to update the passphrase.

When a passphrase is changed, the old passphrase shall not be reused until either:

1. at least four (4) other passphrases have been used, or
2. at least 4 months have passed.

By default, systems shall not display the passphrase in clear text as the user enters it.

Passphrases shall not be stored in script files or function keys.

Passphrases shall always be encrypted for transmission

7.1.5.3 Digital Certificates

Where digital certificates are used for authentication, a revocation process shall exist in case of their compromise.

Digital Certificates that are expired or invalid shall not be trusted.

Owners of systems using digital certificates shall keep their certificates up to date.

Cryptographic implementations should use standard implementations of security applications, protocols, and format, e.g. S/MIME, SSL, SSH, IPsec, X.509 digital certificates. These implementations should be purchased from reputable vendors and should not be developed in-house unless properly trained staff is employed.

All employees shall protect and safeguard any encryption keys for which they are responsible. Private encryption keys shall not be shared with others except when applicable or appropriate

authorities demand that the key be surrendered (i.e. Termination, Promotion, Investigation, etc). While public encryption keys are shared freely, access to the key shall be on a read only basis. Access to digital certificates shall also be on a read only basis.

A test of the validity of a digital certificate shall include the following:

1. The Certificate Authority (CA) signature on the certificate shall be validated
2. The date the certificate is being used shall be within the validity period for the certificate
3. The Certificate Revocation List (CRL) for the certificates of that type shall be checked to ensure that the certificate has not been revoked
4. The identity represented by the certificate — The “distinguished name” is valid (distinguished name refers to the location in the x.500 database where the object in question exists)

A process shall exist in which the current validity of a certificate can be checked and a certificate can be revoked.

Key holders shall initiate key revocation when they believe access to their keys has been compromised.

7.2 Access Control

7.2.1 Least Privilege

All access to computer resources shall be restricted to only the commands, data and systems necessary to perform authorized functions.

1. All data shall have appropriate minimum access privileges, e.g., read, write, modify, as defined by the owner of the data, and shall be maintained in compliance with local laws (some countries have very restrictive laws regarding access to employee information).
2. Access to data shall be restricted to only those individuals and groups with a business need, and subject to the data's classification. Unrestricted/global access should be avoided whenever possible and shall only be used where specifically appropriate and with the data owner's approval.
 - a. An annual review of all resources, e.g., files or directories, to which access is not restricted, i.e., have universal or public access shall be performed and the resource owners shall be notified of the results.
 - b. Common privileges can be assigned to a group of users, but membership to the group shall be restricted to only persons actually performing the given functions. For example, when responsibilities are divided on a geographic basis, the group memberships shall reflect that, i.e., different groups for different geographic regions.

3. All unnecessary services and network services shall be disabled. Any application service which lets the user escape to a shell, provide access to critical system files, or maps/promotes IDs to privileged user levels, shall be disabled.
 - a. An annual review for compliance, which shall be documented including findings, shall be performed. Any findings shall be closed or risk managed.
4. Administrators shall ensure that system access controls, e.g., filters that restrict access from only authorized source systems, are used where they exist and shall only contain necessary system authorizations.
 - a. System administrators shall perform an annual review for compliance, which shall be documented including findings. Any findings shall be closed or risk managed.
5. When not performing specific Administrative Tasks, System Administrators shall use an account with “non-privileged” rights. When Administrative Tasks are necessary, Administrators shall login in using their Administrative account to perform tasks then log back out. If supported by the system, features like “runas” or “superuser” should be utilized whenever possible.
6. Using a shared generic Administrator accounts (i.e. the Default Administrator account) shall not be used except during initial installation or under disaster recovery scenarios. Individuals who require Administrative access shall be assigned unique Administrative accounts where operating systems permit. Please note, an operating system that doesn’t support unique Administrative Access should be viewed as a significant security threat and should be avoided if at all possible. Entities are encouraged to prevent inclusion of such systems onto NG9-1-1 networks unless the mission absolutely dictates it.

7.2.2 Warning Messages

A formal statement of resource intent, i.e., a warning notice, shall be made visible to all those who access Public Safety computer resources and private internal networks. "Welcome" messages, which could be misinterpreted as extending an invitation to unauthorized users, shall not be used.

The login Warning notice shall be issued during the logon sequence (either directly before or after the authentication, preferably before, but it shall be displayed before any substantive data).

All personal computers, workstations and laptops shall display the notice at boot up.

The Warning message shall remain displayed until positive action by the user is taken to acknowledge the message.

The following is an example of a Warning Notice:

Warning Notice

This system is restricted solely to Public Safety authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited by Public Safety. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if monitoring reveals possible evidence of criminal activity, Public Safety may provide the evidence of such activity to law enforcement officials. All users shall comply with Public Safety policies regarding the protection of information assets.

7.2.3 Access Control Measures

Access control measures shall be utilized by all computer resources, systems, applications and networks at all times to restrict access to sensitive information or system/network processors to authorized personnel only. Such measures could include the use of system configuration, file system permissions, system rights or access control software, etc

Where possible access control shall be accomplished with “role-based” privileges that assign users to roles and grant access to members of a role rather than to individuals.

7.2.4 Sensitive File/Resource Access Permissions

Non-privileged users shall not have read/write access to system files or resources such as protected memory, critical devices, executable programs, network configuration data, application file systems, etc. Only users who have administrative responsibilities, e.g., administrators and their designated backups, may be assigned passwords to access and modify these sensitive files/resources.

7.2.5 Rights & Permissions

In order to properly protect a network and, ensure that proper access is given only to those who need it, user rights and permissions must be understood. It is important to understand the difference between a right and permission.

- A right is a property that is assignable to a user or a group, which will either allow or deny them the ability to perform an action. A good example of this is the ability to install a printer on a computer; this is an allowable right that can be assigned.
- A permission, on the other hand, grants or denies access to an object or resource. This would allow a basic user to see only their files while allowing management to see all of the files.

It is also important while implementing these rights and permissions to determine if there are any specific restrictions that need to be enforced, i.e., Law enforcement data can't be shared with Fire/EMS and patient records must be kept confidential consistent with the classification of the data.

The following requirements are provided:

- Access to Files/Folders shall be limited only to those who actually need access
- Home directories, home shares, etc., associated with a User ID shall initially not be readable or write-able by anyone other than the owner of that User ID

- Rights shall be assigned only to those who actually need them and are documented as needing them
- Permissions shall always be configured in accordance with the classification of the data
- Groups should be used whenever possible to simplify administration
- Adhere to the policy of least privileged use, meaning if a basic user can perform all of the tasks necessary, don't grant administrator access to them.
- Rename built in Administrator accounts
- Disable Anonymous or Guest accounts as these typically can be exploited.
- Periodically run audits against users to determine what their effective rights and permissions are. If a user is a member of several security groups it is possible for that user to have elevated privileges that were not intentional.

7.2.6 Separation of Production from Non-Production Systems

For purposes of this document, Production Systems include Training Systems which are intended to become live production systems and therefore shall meet the same criteria as production systems. Production systems (including networking components) shall be separated from non-production systems to ensure the integrity of production data. Physical separation is preferred, but at minimum, logical separation is recommended. If physical separation cannot be achieved then Non-Production Systems must adhere to the same security levels of Production Systems.

Production systems shall not contain any software development tools, such as software compilers and libraries, except where essential for the application. Such tools may be installed during software upgrades or for the installation of new software packages, or for troubleshooting purposes, but shall be removed immediately after their use. Where such tools are essential for production operation, they shall be made inaccessible to users, e.g., placing PERL interpreters in separate directories, not accessible from the web.

Non-production data shall not be transmitted or moved into a production environment without going through proper change control process and receiving authorization, i.e., system/process owner.

Developers shall not be system administrators for production systems for which they have responsibility, i.e., segregation of duties shall exist; except for small stand-alone systems.

Development personnel with a legitimate business need shall only be given access to production systems and data in accordance with, one (or more) of:

1. The system's outage/recovery procedures, e.g., disaster recovery plan.
2. Temporary (time-bound) read-write access when approved via change control.
3. Permanent read-only access.

Any software and/or data changes initiated as a consequence of an outage/recovery procedures or temporary write access shall be documented and retained until it is determined that the production system and data were not corrupted. Production data shall not be copied off a

production system without the service owner's authorization and shall be protected to an equivalent, or greater level.

7.2.7 Screensavers and Inactive Sessions

All devices capable of enforcing a password protected screensaver or a keyboard lock shall do so with the inactivity timeout set to 15 minutes or less, except:

1. When superseded by local Public Safety policy.
2. Users in a customer facing role, such as sales representatives making sales presentations, may have the automated screensaver temporarily disabled so long as the following conditions are met:
 - a. The automated screensaver shall not be deactivated for any longer than justified and not for a period greater than four (4) hours.
 - b. While the automated screensaver is deactivated the screensaver shall be manually activated whenever the device is to be left unattended, even for a brief period of time.
3. Devices that are dedicated to displaying messages/information to a number of people, for example, in a reception area or in an operations center, may have their screensaver disabled so long as the following conditions are met:
 - a. Access (physically and logically) to the device, including its keyboard and User IDs, is controlled in accordance with all applicable physical and logical security requirements.
 - b. Visibility of the display is restricted to only individuals authorized to see the data that will be displayed.

Devices not capable of enforcing a password protected screensaver or a keyboard lock, such as dumb terminals, shall have at least one of the following:

4. Access (physically and/or logically) to the device, including its keyboard and User IDs, controlled in accordance with all applicable physical and logical security requirements.
5. The console is configured to automatically logout after 15 minutes of inactivity (This is not to terminate running commands).
6. Have session inactivity timeouts set for 15 minutes.
7. Users logout when console is left unattended if automatic inactivity logout is not supported

<p>NOTE: The time taken by network components to allow firmware or software updates to complete is not to be considered a period of inactivity.</p>
--

Hence, personal computers utilizing the operating system's screensaver typically does not need to have their applications include inactivity logic.

7.2.8 Future Communication Services

Public Safety is a mission critical production environment. Security assessments shall be conducted for any new form of communication that wants to be added or linked to a NG9-1-1 environment. Only after sufficient security control is in place can such new forms of communication can become connected. The following sections provide best practices and recommendations for securing such new forms of communications.

7.2.8.1 Business and Security Risks

Before the traditional security enforcement and deployment of new forms of communication, a risk assessment should take place, the followings shall be considered by the public safety community as business risks:

1. the resource availability impact,
2. business justification or importance of the service or data to use a specific communication method (the utility of the service compared to the security risk),
3. false-positive rate (e.g., the possibility this new form of communication can generate false alarms while there are no security vulnerabilities),
4. false-negative rate (e.g., the potential of unknown new vulnerability is introduced by this new technology while the vulnerabilities are undetected),
5. legal status (e.g., liability, contract language, recording as evidence, authority to access information, privacy protections),
6. volume (normal, bandwidth, latency, diversity/redundancy induced denial-of-service, etc).

Business risk (of the public safety community) acceptance shall not be the charter of the security function.

7.2.8.2 Communication Partners and Scope

Beyond technology, the users using new forms of communication can be confined by their realms (for the purpose of this document a realm is a network or service with specific security characteristics). One realm may or may not be allowed to communicate to other realms. More importantly, some realms may not be trustworthy. For example, a known email service provider where 97% of the emails originated/relayed from that realm are spam emails, unchecked email senders, or virus-infected.

The scope definition may be controllable by creating a communication partners white-list. Be aware such a list may also be a “moving target”. Selection of a reputable, experienced service provider is highly recommended because a seasoned service provider usually knows how to keep up with the most recent “security climate”. A good service provider may even declare an emergency to temporarily block the gateway to its peering partners to confine the risks when it detects an outbreak of security events pertinent to its service.

7.2.8.3 Information Delivery Service Demarcation

The new forms of the communication methods may be performed by one or multiple-cascaded¹ service providers. Some service providers may even perform the format conversion function as a gateway in between the new format and the legacy format.

Example 1, an IP-enabled Telecommunications Device for the Deaf (TDD) service provider may have one listener side on the IP space while its output is the standard legacy TDD circuit to the TDM world. In this example, the demarcation from NG9-1-1 Entity point of view is still the traditional TDM switch, not anything related to TDD-IP.

Example 2, a VoIP Gateway “Wholesale” Clearing House is performing a VoIP gateway function² for the entire NG9-1-1 Entity communication, i.e., put the shareable functionalities/new technology in the cloud, then feed and serve individual NG9-1-1 Entity as a “virtual facility” using the traditional/legacy communication method.

These may be the potential new service provider models and their demarcation and associated roles/responsibilities/SLA will be different than NG9-1-1 Entity’s own. On the other hand, if such function is performed within the NG9-1-1 Entity (by NG9-1-1 Entity itself or by a service provider within), the responsibilities will “move”, since the demarcation might have moved.

7.2.8.3.1 Client Software Add-ons (“Plug-ins”) Security Risk

Many add-on or plug-in features are not needed and occasionally become a security risk. For example, browsers may allow a new “software plug-in” (i.e. Flash, Shockwave, Java, etc) to be installed without its true intent being identified (a worm, a key-logger, a Trojan to steal database content). Another example is a piece of software may allow a file being transferred into or out of the NG9-1-1 Entity environment without any form of approval. The arbitrary installation of plug-ins can potentially cause security risks to the NG9-1-1 Entity.

Therefore, all client software installed in NG9-1-1 environment shall be approved, inventoried and audited for compliance, including appropriate version. Client software shall not be configured to auto accept the software add-on or plug-ins.

Compliance checks shall occur in concert with the audit schedules defined in section 11 of this document.

All new add-on software or plug-ins shall be tested before installation.

It is noted that many tools exist that can be used by NG9-1-1 entities to assist in the automation and policy enforcement of software add-ons, etc.

¹ intermediary service providers in the delivery chain

² In one of the NENA proposal, it seems to be the direction they are advocating.

7.2.8.4 Peer-to-Peer Networking

Peer-to-Peer (P2P) Networking has become quite popular since it leaves the “central server and the potential for its control” out of the picture. For example, in a music-sharing application, the central server just serves as the indexing function, i.e., answer one client’s question: “who has the music collection by the name Happy Birthday”, once the answer is given, the central server is out of the picture (the P2P service provider attempts to avoid legal liability/lawsuit especially from content/title holders.) Then the File Sharing part of client software kicks in using UDP to talk directly to another computer who claims it has that piece of music. P2P’s software client is well-known to be infected with Trojans and its “business need” list is nil.

The P2P solutions that exist today are unsuitable for use in NG9-1-1 environment. This may change but until such time as reasonable IT Security standards for P2P are adopted, P2P shall not allowed in the NG9-1-1 environment.

7.2.8.5 Hybrid Communication Method: VoIP

NG9-1-1 entities might already run one form of VoIP (i.e. County VoIP system). Security becomes an issue when another VoIP realm needs to communicate with another VoIP system within the NG9-1-1 Entity. From security point of view, this becomes the question of how to securely interface with other realms.

The NG9-1-1 Entity should not connect its own system with others (i.e. connect the NG9-1-1 VoIP system with the County’s VoIP realm) without securing the connectivity.

7.2.8.6 Telecommunications Device for the Deaf (TDD)

The security of legacy TDD devices and communication methods is outside the scope of this document.

Future advancements for emergency services communication in the hearing and speech impaired community may require security requirements to be established at a later date.

7.3 Confidentiality

7.3.1 Disclosure of Information

As noted in this document, all information shall be classified and handled appropriately. However, some information captured by the NG9-1-1 Entity may fall into the public domain and be either discoverable or otherwise requested by the general public or media. Data falling into this category shall be clearly identified and specific guidelines written and followed to document what data is released, when and to whom. Further, these guidelines shall capture any specific release requirements for data such as video, names, call content, message text or other personal content. Where such data is intermingled with other data of differing classification, consideration shall be given to replicating the public domain data into a separate data store.

7.3.2 Email Security

Future NG9-1-1 deployment models may leverage or utilize email based emergency communication systems. It is important to understand that email based emergency notification systems are viewed by this document as different from a NG9-1-1 Entity's internal email system.

The use of email in any scenario should be done with caution. It is recommended that internal NG9-1-1 Entity mail not be made available on a 911 call-taking position workstation but rather on a separate system. However, email based emergency communication systems shall be allowed with appropriate security mechanisms. NENA has not defined email security standards in this release of the document, but may do so at a later date. In lieu of standards NG9-1-1 entities are encouraged to follow best practices such as those offered by the National Institute for Standards and Technology (NIST)

Additionally, personnel who use electronic mail systems to send NG9-1-1 Sensitive information shall implement appropriate security controls to assist them in protecting incoming and outgoing messages. The originator of an email message containing Proprietary information should ensure that:

- The message is clearly marked to reflect its proprietary classification.
- The email ID to which the information is being sent is correct.
- The recipient of the email message understands the safeguards associated with the proprietary marking. The originator of the email message may have to explain the safeguards to the recipient of the email message in advance.
- If printed, the email message shall be protected according to the rules associated with its proprietary marking.
- The proprietary information is encrypted in accordance with NG9-1-1 Entity requirements.
- Internal mail shall not be automatically forwarded out the internal network, such as via the Internet, to any other mail system.
- NG9-1-1 Entity employees and contractors shall only use a NG9-1-1 Entity domain email address to conduct business unless otherwise obligated to do so through a formal contractual document.
- NG9-1-1 Entity database systems which are used to define the contact details for personnel performing work on behalf of NG9-1-1 Entity shall only contain email addresses within NG9-1-1 Entity domain unless covered by contract.

7.3.2.1 Text Messaging

Individual messaging services, e.g., SMS, need to be evaluated to ensure the service characteristics, service grade, contract language, and security posture can meet NG9-1-1 Entity production and security requirements.

7.3.2.2 Video-Clip Multimedia Messaging

In mobile phone services, there is a multimedia messaging service (e.g., MMS) which allows “video-clips” being captured by the mobile device to be sent to the recipients, similar to SMS message delivery scheme except that the content is enriched. The source of the multimedia material is the cellular phone’s own camera but due to technological advancements such technology could be falsified or obtained from video sources e.g., Internet posted, PC edited “video productions, etc. For such service to be considered as an acceptable (authenticity, secured, and valid) data feed for NG9-1-1 Entity, it needs to be evaluated to ensure the service characteristics, service grade, contract language, and security posture can meet NG9-1-1 Entity production and security requirements. These can be independent efforts and are out of scope of this document and/or may be addressed in a future release.

7.3.3 Encryption and PKI

7.3.3.1 Encryption Algorithms

Cryptographic implementations shall use industry standard cryptographic algorithms and standard modes of operations. It is recommended that the algorithm certified by the US National Institute of Standards and Technology’s (NIST) FIPS 140-1 certification, currently AES, be used. More information on current US federal encryption standards and modes of operation is available from the NIST Computer Security Resource Center.

Where there are no applicable US federal standards for specific encryption functions, e.g. public key cryptography, message digests, commercial algorithms may be used, e.g. RSA, Diffie-Hellman, RC4, and SHA-1. Implementations and modes shall follow best commercial practices, e.g. Public Key Cryptography Standards. Implementations and modes shall use the strongest available product. More information is available at:
<http://www.rsasecurity.com/rsalabs/pkcs/index.html>.

The use of any encryption algorithm or device shall also comply with the laws of the United States and those of any country in which there are plans to use data encryption.

7.3.3.2 Key Lifecycle Management

The current state-of-the-art in information security relies upon Public Key Cryptography. Simply put, Public Key Cryptography uses pairs of keys to lock and unlock data. When Public Key Cryptography is used to securely send data, one key, the private key, can only unlock the data, while another key, the public key can only encrypt data. This means that the public key can be freely distributed.

If Bob wants to securely send data to Mary, he can look up Mary’s public key, and use it to encrypt the data. Once this is done, only Mary’s private key can decrypt the data. As long as the private key is kept secure, Public Key Cryptography is very safe. Since the private key is never exchanged, keeping the private key safe is easily done. There is no need to secure the public key since it cannot be used for decryption. This makes it easy to distribute the public key to those

who want to securely send information. To efficiently implement Public Key Cryptography, a Public Key Infrastructure (PKI) is used to manage and distribute the public keys.

For both Symmetric Key and Asymmetric Key cryptography, management techniques shall exist to manage the lifecycle of the cryptographic keys, such as creation, distribution, validation, update, storage, usage, and expiration.

All personnel shall protect and safeguard any encryption keys for which they are responsible. Private encryption keys shall not be shared with others except when NG9-1-1 Entity demands that the key be surrendered. While public encryption keys are shared freely, access to the key shall be on a read only basis. Access to digital certificates shall also be on a read only basis.

Encryption devices and any server used for storage of encryption keys shall be protected from unauthorized access.

Key generation shall be performed using commercial tools that comply with x.509 standards and produce x.509 compliant keys. Keys shall not be generated or derived from predictable functions or values, e.g. values considered predictable include user identity information, time of day, stored/transmitted data.

Symmetric keys shall be at least 112 bits in length.

Asymmetric keys shall be at least 1024 bits in length. However, this shall be increased to 2048 bits where feasible.

Keys, whether symmetric, secret keys or PKI based key-pairs, shall be expired and new keys generated in accordance with industry acceptable practices. Decrypting keys may be revoked at any time if a responsible employee or NG9-1-1 Entity believes the key has been compromised, or if the NG9-1-1 Entity no longer employs the person assigned those keys.

Keys shall only be distributed to appropriate recipients through secure channels. Keys used for encrypting stored data shall be safeguarded so that authorized persons can recover them at any time in order to recover NG9-1-1 Entity data or information

7.3.3.3 Public Key Infrastructure

The use of a Public Key Infrastructure (PKI) is encouraged to support applications (e.g. secure email and SSH) that need encryption, authentication, and signing functions.

Any PKI that is used or implemented shall have a documented Certificate Practice Statement (CPS) that defines how security is provided for the infrastructure, the registration processes, relative strength of the system, and legitimate uses of the infrastructure. Hence, the CPS ensures that the PKI provides appropriate services and protections necessary to meet the needs.

A PKI shall implement a registration process that verifies the identity of a digital certificate requestor using an acceptable form of identification prior to the CA creating a digital certificate that binds the requestor's identity to the public key provided. The choice of acceptable form of identification shall be based upon the level of trust required within the PKI. If a high level of trust is required, then a possible form of identification may be a Photo ID, e.g. passport. The

choice of process shall also consider the strength of the private key protection for certificate holders.

A process shall exist in which the current validity of a certificate can be checked and a certificate can be revoked.

Key holders shall initiate key revocation when they believe access to their keys has been compromised.

7.4 Integrity

7.4.1 Obtaining Files or Software

All files and software shall be obtained from trusted sources, and shall be scanned for viruses and malicious code. Any binary or executable files obtained from un-trusted sources, shall be verified to be free of logic bombs or other malicious code before being used.

Freeware, Shareware & Open Source software shall be obtained from a reputable source, e.g. Public Software Library (PSL). If obtained from non-trusted sources such as Internet web sites, it may not be used on NG9-1-1 Entity computers unless authorized by management.

7.4.2 Maintaining Accurate Time Reference

Time synchronization shall be in accordance with the NENA 04-002 NG9-1-1 Entity Master Clock standard.

7.4.3 Computer Viruses and Malicious Code

Any device used to conduct business that is capable of running anti-virus (sometimes now called anti-malware) software shall have that software installed, running and up to date to protect from virus infection. The essential trustworthiness of the software used to conduct NG9-1-1 Entity business shall be maintained, i.e., kept free of viruses and other malicious programs.

Personnel, including all contractors with current service agreements, shall:

1. Install and maintain the latest version (including engine) of the licensed anti-virus software.
2. Update servers and workstations, including personally owned equipment used for business, with the latest version when made available.
3. Antivirus software shall be current with the latest available and applicable virus definition files
4. Scan all files when opened and/or executed (including files on network shares).
5. Scan all files on all local drives at least once a week.
6. Scan all files, attachments and software received via email and/or downloaded from web sites before opening and/or executing.
7. Scan all removable media and software (including new workstations equipped with pre-loaded software) before opening and/or executing.

8. Scan all removable media and software before opening and/or executing if it has not been kept secure within your control.

Additionally, server administrators shall scan all files made available as network shares at least once a week.

7.4.4 System Changes

Any changes to computer system hardware and operating system software shall adhere to the following:

1. Formal documented procedures shall exist and be followed.
2. Appropriate level of authorization shall be required and obtained prior to change(s).
3. The Administrator shall control software changes that affect the operation of an application, operating system, or utilities. This includes updates and upgrades that could affect user response, machine performance or operations, security, or system availability.
4. A detailed audit trail of all modification to network hardware and software shall be created, retained and reviewed at least annually.
5. Records of all system/application changes should be retained for a minimum of three years and in no cases less than 1 year or the last major upgrade whichever is longer.
6. System Controls shall indentify accountability for all program changes to a specific programmer, and approving manager.
7. Exception reporting procedures shall be built into system software to detect computer, program, communications, and operations failures. Error checking and validation controls shall be in place, e.g., checksum monitoring, to validate the integrity of the data.
8. Ensure current backups provide the capability to recover in the event of system problems created by the changes.
9. In cases where system administration or maintenance is outsourced, all records kept by such agencies shall be available to the NG9-1-1 Entities to review.

7.4.5 System Patching

Vendors and security organizations issue either alerts or advisories relating to security flaws that allow unauthorized access to systems or data, to bypass access controls, or gain unauthorized privileged authority as they are discovered in operating systems and other software. All available and applicable vendor-provided patches that address critical security vulnerabilities and have been approved by management for use shall be applied as quickly and prudently possible. Testing of patches is strongly encouraged.

NOTE: During a virus outbreak, such as Code Red, Blaster, or Slammer worms, as soon as the NG9-1-1 Entity Security Risk Manager, Security POC / Team, or authorized agent acting on behalf of a NG9-1-1 Entity receives a **critical** level alert from a centralized Security Advisory authority, action shall be taken immediately to address the risk. **A critical risk may require implementation of emergency measures.** These measures may include applying patches immediately and preparing to operate the NG9-1-1 Entity in a diminished mode. Examples of alternative operation modes can be:

- route 911 traffic to an isolated and hardened NG9-1-1 Entity
- raise firewall to prevent further spreading of virus/worm
- re-direct calls to an administration work station
- exercise emergency restoration options

Procedures shall be instituted which verify and document that the business hardware and software are currently supported by the manufacturer or supplier such that advisories are issued and fixes are made available for any newly discovered security vulnerabilities.

Where possible, permanent fixes shall be used in preference to temporary fixes. However, where a temporary fix (work-a-round) is advised and a permanent fix is not available, the temporary fix shall be used within the prescribed timescale until a permanent fix becomes available.

A process shall be in place to ensure that all applicable permanent fixes are installed, and that temporary fixes cannot become disabled until the permanent fix has been installed.

All fixes (temporary or permanent) shall be tested prior to using them in a production environment. Testing shall also be done to ensure that no security vulnerabilities are introduced, e.g., unnecessary services or default User IDs re-enabled.

7.4.6 Server and Workstation Configuration

Servers, End-users workstations, desktops, or laptop PCs shall be hardened (i.e. unused services disabled, and no “local administration right” is given to the end-user, etc). Any exception shall go through the applicable approval process. NG9-1-1 entities should follow recognized best practices for Operating System hardening like the National Institute for Standards and Technology (NIST) guidelines or the ISO 27002 standards.

In a few cases, e.g., Business Continuity/Disaster Recovery during emergency evacuation, laptop PCs (e.g. call-taker position, CAD, MIS PCs) may be moved from one NG9-1-1 Entity to another NG9-1-1 Entity. During the transit, these machines’ configuration shall not be changed. Unless explicitly approved, these machines shall not be used/powered on during transit.

In this document, virtual office³ workstation/PC arrangement, either using NG9-1-1 entity provided PC or personally owned PC, is not recommended due to the high sensitive nature and high reliability requirement of the NG9-1-1. However, if properly secured this model along with Virtualization may be a viable option as newer technologies to secure this information in this environment are developed and implemented.

7.5 Availability

There is often an extremely high cost associated with achieving 100% uptime availability. The realistic goal is to achieve *near*-zero down time. It is at the discretion of each NG9-1-1 Entity to weigh cost and security against availability to achieve the desired balance and/or set the applicable level of targeted uptime.

Critical and non-critical services may have different availability levels. While some services are difficult to duplicate other services may be temporality augmented or reduced. For example, if the ALI linked CAD is not functional; a manual lookup method allows the equivalent. This is a slower method, but the service is still available. Another example would be if the ALI or map is not available, E911 service would be temporarily degraded to basic 9-1-1 service.

7.5.1 Security Impacts to Availability

Security functions are required to deter the intentional or unintentional attacks from an environment outside the NG9-1-1 Entity, from reaching into the NG9-1-1 Entity's inside perimeter causing damage and outage. Security measures shall be as transparent as possible and should not be an insurmountable burden in achieving high availability.

Redundant links, backup connection using on-demand dialing, or other arrangement can be chosen for increased link reliability.

From a security work function point of view, the two main security goals shall be:

1. Fulfill security tasks while maintaining the availability of the NG9-1-1 Entity.
2. Perform maintenance tasks while retaining supportability and administrative functions.

The security design shall make the environment serviceable and all possible failure scenarios shall have the corresponding actions pre-planned.

7.5.2 On-Site/Local High Availability

Building high availability in networks can be handled by multiple elements such as:

1. Redundant LAN switches

³ E.g., working from home arrangement

2. Teamed⁴ NICs in servers and mission-critical desktop computers
3. Redundant servers
4. High availability or redundant firewalls
5. Redundant routers
6. Redundant WAN links
7. Out-of-band communication links
8. Redundant management LAN/WAN
9. Remote control board for servers
10. RAID arrays
11. Dual-CPU and/or other high-available server designs
12. Redundant premise wiring
13. Redundant HVAC

The goals shall be:

1. Any single point of failure is identified and the alternative strategy is planned and documented.
2. Distribute the down-time window, if possible. For example, if an approved security patch is about to be applied to a server farm, apply them in the proper order such that at minimum one server will still be in production while others are being patched/rebooted.
3. All equipment shall be managed and monitored such that if one of the high availability elements is already down, the status shall be made known to the NG9-1-1 Entity and the management entities. Authorization for expedited service and the associated costs should be considered.
4. Plans shall be thoroughly tested and documented. Annual drills shall be exercised and post-mortem analysis and action plans produced.

7.5.3 High Availability by Geographic Redundancy

Local high availability may not cover all failure scenarios and may not work all the time. It may be necessary for a back-up facility to temporarily assume work functions. This may be required for NG9-1-1 Entity functions, service provider functions or possibly both.

Geographic redundancy shall be pre-planned, be it a partner or mutual-support NG9-1-1 Entity, or a service provider's alternate data center. The communication path shall be re-routed in an acceptable and pre-defined timeframe.

⁴ NIC teaming is a technology offering two separate paths into the same server where only one IP address is known to the local area network.

The fail-over scenarios shall cover trigger-driven events (e.g., threshold crossing) as well as pre-scheduled events (maintenance downtime). Fail-back criteria shall also be defined such that a smooth transition back to normal production arrangements can take place.

7.5.4 Backup/Restore and System Recovery to a Secure Condition

Operationally, the NG9-1-1 Entity and its suppliers/service providers shall have a strategy to deal with system failures. Backup storage media may be magnetic media, optical media, etc. Note that the actual storage may or may not reside in the same physical location as the operational systems. A backup and rotation schedule should be established. Backup media should be securely stored. If restoration is needed, sufficient care shall be taken such that during restoration, sensitive information will not be leaked out or privileged information (e.g., root or Administrator password) will not be disclosed. A copy of the routine full backup media shall be sent to a secure offsite location for archiving and Disaster Recovery (DR) purposes.

7.5.5 Business Continuity and Disaster Recovery

The high availability design shall cover the normal course of a NG9-1-1 Entity's production scenarios based on reasonable time-and-cost assumptions. There are other scenarios which are beyond normal situations, (e.g., wars, major catastrophic, etc). Under such situations, Business Continuity and Disaster Recovery (BC/DR) mechanisms⁵ may be invoked. BC/DR plans shall be created but this is beyond the scope of this security document.

However, NG9-1-1 Entities are reminded to take the entire network operating requirements into consideration when developing Business Continuity and Disaster Recovery plans. A worst case scenario should be assumed; you are not functioning and neither is anybody else in the immediate area. Recovery within 50 miles of your current location is highly unlikely. Plans should be made for a distant recovery site.

BC/DR drills shall be conducted periodically within a fixed interval to be defined by local policy and minimally on a per annual basis.

7.6 Audit and Accountability

Systems, including but not limited to applications and databases, shall have internal controls for logging, tracking and personal accountability.

7.6.1 Security Audit Logs

Systems, including but not limited to applications and databases, shall have a security event record (log) mechanism that is capable of providing information sufficient for after-the-fact investigation of loss, impropriety or other inappropriate activity. A system, or if necessary, a

⁵ E.g., use alternate communication method such as Ham radio, WAAS radio, cellular phones, emergency broadcast system, etc.

group of interacting systems, shall have end-to-end logging capability sufficient to substantiate user accountability for all significant events within the system and among the interacting systems. A log collector product or process shall be used to periodically retrieve the data from the target systems and archive them outside of the original systems creating the log events.

All resources to which access is controlled including applications and operating systems shall have the capability of generating security audit logs.

All security logging mechanisms, e.g., UNIX® accounting, shall be active from system initialization. These mechanisms include any automatic routines necessary to maintain the activity records and cleanup programs to ensure the integrity of the security audit/logging systems.

7.6.2 Security Audit Log Review

Administrators shall develop and document a security audit log review plan to include:

1. the frequency for security audit log review based upon such criteria as: criticality of the system, business risk, cost, system classification, and
2. the minimum unusual activities to be reviewed for, these might include for example: multiple unsuccessful login attempts, user attempts to access files or resources outside their privilege level, network activity.

Where the security audit log review is automated, anomalies in the security audit log shall be alarmed.

7.6.3 Security Alarms

Administrators shall develop and document a security alarm plan to include:

1. the undesirable events such as potential security problems or suspicious activity for which security alarms shall be generated, e.g., high volumes of bad packet data, corrupted data, attacks, or information gathering attempts.
2. the threshold levels for these events. These shall be set so as to detect events that might impact the service, enabling action to be taken, while not resulting in an excessive number of false alarms.

At a minimum, security alarms shall be activated automatically by the following events:

3. Six (6) consecutive unsuccessful login attempts.
4. Successful modification of critical system or application files (as defined by the administrator).
5. Unsuccessful attempts to gain permissions or assume the identity of another user.

8 Physical Security Guidelines

All NG9-1-1 Entity information resources shall be kept physically secured and protected from theft, misappropriation, misuse, unauthorized access and damage.

8.1 Building and Physical Access Control

1. Doors with security mechanisms shall not be propped open.
2. Employees, suppliers, contractors and agents authorized to enter a controlled physical access area shall not allow unidentified, unauthorized or unknown persons to follow them through a controlled access area entrance.
3. Each person entering a controlled access facility shall follow the physical access control procedures in place for that facility.
4. Personnel shall be vigilant while inside the building and challenge and/or report unidentified persons including persons not displaying identification badges who have gained access.
5. When automated access control and logging devices are installed, personnel shall use them to record their entry and exit.

8.2 Authorized Physical Entry

8.2.1 Resident and Recurring Non-Resident Authorized Entry

All building residents and other persons authorized for recurring, unescorted entry into a NG9-1-1 Entity facility that houses information resources shall be permitted entry only in accordance with the following paragraphs.

Physical access control devices issued to an individual shall never be loaned to, or shared by, another person.

A person possessing an access control device shall never use that device to allow access to an unauthorized person.

8.2.1.1 Non-Employees

Non-employees who are to be issued NG9-1-1 Entity identification badges, building access cards, building keys, and/or any other form of recurring access that does not require approval at the time of access shall be sponsored by a NG9-1-1 Entity management person.

Appropriate local, state and federal laws and guidelines shall be followed for allowing non-employee access (i.e. CJIS Background Checks, etc).

8.2.1.2 Identification Badges

Identification badges containing a picture of the holder shall be issued to all residents of buildings containing information resources.

If the facility is guarded, the identification badge shall be displayed to the guard upon entry into the facility.

Identification badges shall be displayed by a person at all times while in a NG9-1-1 Entity facility and/or on NG9-1-1 Entity premises.

A person on NG9-1-1 Entity premises shall present his/her identification badge for examination and/or verification upon request. Failure to comply may result in removal from the facility and/or denial of further physical access to the facility.

Building residents and non-residents with recurring access authorization who do not have a valid identification badge in their possession shall be signed in and vouched for by an authorized building resident who possesses and displays a valid picture identification badge.

A temporary identification badge shall then be issued and the number of the badge recorded on the sign-in log along with the identity of the person vouching for the entry.

Possession of a temporary identification badge does not constitute permission to reenter a building. Identification, sign in and authorization procedures shall be followed.

A temporary badge shall be returned when the person leaves the building.

Lost or stolen identification badges and/or building access keys or cards shall be reported to the ENTITY that issued the badge, key or card.

8.2.2 Entry by Others

Persons holding any NG9-1-1 Entity picture identification badge shall display this badge at all times while in/on the site.

All those requiring non-recurring entry shall be signed in by a person who displays a valid NG9-1-1 Entity picture identification badge that authorizes that person entrance into the site. A temporary identification badge shall then be issued to the visitor and the number of the badge, the person's name, the date and the name of the person authorizing the access shall be recorded on a sign-in log.

The person shall display the temporary badge at all times while on NG9-1-1 Entity premises.

All temporary badges shall be returned when leaving the building and the log shall be noted accordingly.

All visitor temporary identification badges shall have the words "Escort Required" prominently displayed. Persons displaying temporary identification badges with the words "Escort Required" and who are not escorted shall be removed from the building.

Lost temporary identification badges shall be reported immediately to the ENTITY that issued the temporary badge and attempts shall be made to recover the temporary badge.

Possession of a temporary identification badge does not constitute permission to reenter the secured area for which the badge was issued. Identification, sign in and authorization procedures shall be followed.

8.3 Storage Media and Output

Data stored on removable media that is external to the system hardware such as diskettes, tapes, cartridges, USB memory devices, and Optical Media shall be safeguarded.

Personal storage devices (i.e. user owned USB thumb drives, etc) shall not be used.

Sensitive data shall be printed on an attended printer or one in a secured area. Distribution of the output shall be controlled. Printouts containing sensitive or critical information shall be kept in

All printouts containing classified information shall be protected.

When producing copies of printouts containing classified information, the originals and/or copies shall not be left unattended at the copier.

Storage media and output (e.g. CDs, tapes, diskettes, hard disk drives, printouts, memory chips, flash drives) shall be destroyed in such a manner that the contents cannot be recovered or recreated

NG9-1-1 Entity personnel shall ensure that re-used storage media is “clean”, i.e., does not contain a residual of information from previous uses.

All media distributed outside NG9-1-1 Entity shall be new, or come directly from a recognized pool of “clean” media.

8.4 Mobile Devices

8.4.1 Security in the Work Area

All portable computing devices, including, but not limited to laptops, Personal Data Assistants (PDAs), data backup/storage devices, communications devices, testing devices, monitoring equipment and authentication devices, shall be kept physically secured as denoted below:

- When equipped with locks, portable computing devices shall be kept locked to prevent theft. Keys shall be stored in a secured location.
- Docking station style portable devices shall be locked in a secure location (i.e. File Cabinets, Safes or Desks) when not in use. Docking station style portable computing devices shall not be left unattended outside normal business hours even when in the docking station.
- Other portable devices shall be stored in a locked cabinet, drawer, or office (not just the building) when not in use.
- Extra security precautions shall be implemented in and around the receiving, staging, assembly and storage areas used for large deployments of portable computing devices.

8.4.2 Security Outside the Work Area

- Portable computing devices shall be secured when unattended (i.e. in hotel and meeting rooms). Use locking cables and/or other restraints whenever possible.
- Portable computing devices should also be concealed from view whenever possible when unattended.

- Computers shall not be left in view inside unattended vehicles.
- Vigilance shall be maintained in airport luggage inspection and transfer areas, hotel check in and check out areas, and other public areas.
- Devices shall not be left unprotected in conference rooms, etc.
- If possible, information resources using a power supply shall be connected to electrical outlets and communications connections that utilize surge protection.
- Devices shall not be exposed to extreme heat or cold.
- Whole disk encryption should be used whenever possible.

8.5 Environmental Controls

Information resources shall not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions shall also be taken to ensure that information resources cannot be affected by problems with utilities, such as water, sewer and/or steam lines that pass through the facility.

All information resources shall be protected from damage caused by spills, etc., from food or drinks.

At a minimum, all buildings housing significant NG9-1-1 Entity information resources shall have a documented fire plan, smoke and/or fire detection devices, sprinklers or other approved fire suppression systems as required by local code, and working fire extinguishers in easily accessible locations throughout the facility.

Information resources using an electrical power supply shall require UPS or surge protection as noted below:

If the information resource is critical to business operations, a UPS shall protect the information resource or the processing performed shall be duplicated or mirrored in a second location not generally subject to the same power outage.

All buildings containing critical information resources shall have protective physical measures in place. Physical access to other critical support facilities in the immediate area of the center shall also be protected. This includes locking manholes containing communications, electrical power, water, and natural gas facilities.

8.6 Server Room

Server Rooms, which may include Data Centers, Wire Closets or the Backroom, house critical information resources like servers, switches, routers, PBXs, wiring termination points, etc.

Note: The security requirements noted herein are designed to highlight important and relevant security aspects but should not be viewed as a comprehensive list on how to build a data center or server room, etc.

8.6.1 Physical Access

Entry to the Server Room and the following listed Server Room support facilities shall be restricted to personnel having a true business need for physical access.

1. Commercial power rooms
2. Emergency power rooms
3. Communications rooms
4. Cable vaults
5. Switch rooms
6. HVAC equipment rooms
7. Operations control rooms

NOTE: This paragraph applies to the Server Room, not necessarily the entire building which houses the Server Room.

All entrances and exits to the Server Room shall be controlled by a security system. Acceptable methods for controlling entry include guarded entrances, keyed physical access cards or keyed locks. The physical access controls shall be effective 24 hours a day, seven days a week.

Raised floors and suspended ceilings shall not allow physical access from outside the Server Room. Card readers and/or biometric devices should be used whenever possible to control access and record exit through all doors to the center.

8.6.2 Damage Control

The following controls shall be present in the Server Room:

1. Fire protection/detection systems, as required by code or internal NG9-1-1 Entity standards, shall be maintained and inspected at regular intervals. This includes, but is not limited to clean agent suppression systems, sprinkler systems, occupant hose systems, fire extinguishers and early warning fire detection systems.
2. If sprinkler systems are provided, fire retardant polyethylene sheeting shall be readily available for protecting media and equipment.
3. In other cases where water may be used for fire suppression or other water damage is possible, fire retardant polyethylene sheeting shall be readily available for protecting media and equipment.
4. Equipment cooling systems shall be installed and in good working order. Water sensing devices with alarms shall be positioned near valves of the cooling systems and other places where water is present.
5. Heating, ventilating and air conditioning (HVAC) systems shall be utilized to maintain the environmental conditions within the range required by the manufacturer of the systems equipment. There shall be dedicated HVAC system for the Server Room.
6. All critical information resources shall be on a UPS.
7. No food or drinks shall be allowed in any NG9-1-1 Entity Server Room.

8. No smoking is allowed in any NG9-1-1 Entity Server Room.
9. Storage of material under raised flooring is prohibited.
10. Storage of combustible material in the center is prohibited.
11. Furniture, storage cabinets, and carpeting shall be fire retardant.
12. Carpeting, if used, shall be anti-static carpeting.

8.7 Data Communications Networks

All data communications network elements shall be secured to the extent practical. Specific requirements must include, but are not limited to:

1. Hubs, routers, repeaters, bridges, firewalls, modems, ISDN bridges, network management consoles, patch panels, and other similar equipment shall be contained in locked rooms with appropriate physical access controls. If equipment is located in equipment rooms shared with non-NG9-1-1 Entity entities or in unsecured space, it shall be contained in locked cabinets.
2. Active network jacks and connections shall only be located in physically secured locations, i.e., NG9-1-1 Entity owned or leased space, in locked cabinets, or protected by locked physical barriers.
3. Unused network connections shall be removed or disabled in a timely manner.
4. Network media shall be selected and located so as to discourage wiretapping, electronic eavesdropping, or tampering, where feasible. This would include the use of fiber optic cable, coax, and/or enclosed conduit for cable runs.

9 Network and Remote Access Security Guidelines

This section addresses a number of security issues and risk mitigation strategies for networks in the NG9-1-1 Entity environment as well as connections allowing access into and out of those networks. These guidelines anticipate the very critical nature of the NG9-1-1 Entity mission and its importance to the general public for access to emergency services. The mission critical nature of the NG9-1-1 Entity is also discussed in the first section of this document.

9.1 Firewalls/Security Gateways

The NG9-1-1 Entity responsible for the network shall identify and classify network segments (e.g., call taker networks, CAD networks, etc) based on their business and technical functions so that the appropriate levels of protection can be configured for each segment. All boundaries or points in ingress and egress shall be clearly defined for every network. These may include external network connections, dual homed servers or other points of contact with other networks of different classification.

Firewall implementation guidelines shall include:

1. Firewalls shall be established at all boundary points to control traffic in and out of the network. All firewalls shall utilize a “fail all” final rule by default. Traffic shall be limited in both inbound and outbound directions by rules which specify source and destination addresses and destination ports. Stateful Packet Inspection firewalls shall

- be the minimum firewalls supported however, Application Layer Firewalls are strongly recommended. Simple “router” ACL rules are not sufficient as a “firewall.”
2. As part of the implementation of any firewall administration process, clear guidelines shall be established which indicate what services are permitted between endpoints. Since the base firewall policy is defined to be a “fail all” policy, no service shall be allowed without restriction on a perfunctory basis. (Note that a “deny all” policy, also known as a “white list” policy blocks all traffic by default.) However, access can be considered by the firewall administrator when presented with a business need request for the service. Such changes must be managed through a documented Change Control Process. The firewall administrator shall retain the right to escalate any such request via a documented escalation process if in disagreement with the request
 3. Firewall rules generally consist of source and destination addresses and source and destination ports. In general, when an exception to a “deny all” rule policy is considered, these parameters shall be as tightly controlled as possible. At a minimum, restriction of source and destination IP addresses shall be specific to individual addresses. If more advanced technologies offer equivalent or better protection, they can be used. In some occasions, subnets or network ranges may be considered, but the security risks for every host or platform within the network range or subnet shall be evaluated.
 4. The firewall administrator shall seek to minimize the number of ports exposed or permitted through the firewall.
 5. All firewall administrators shall be highly qualified and experienced. Qualifications which shall be considered would include industry and/or vendor certifications with various firewall products. Additionally, the firewall administrator shall have an in-depth knowledge and/or experience in firewall support and management, various operating systems including application and operating system protocols (ports and sockets) and associated security implications. Other essential skills shall include networking, routing, LAN/WAN technologies and related security considerations.
 6. Use of ports required by operating system or infrastructure functions and features across network boundaries shall be strictly controlled at the firewall. Examples include ports associated with NetBIOS, Directory Services, and file sharing.
 7. All rules shall be reviewed periodically and at least once annually to verify continued need
 8. Firewalls shall be assessed at a minimum of annually to address any service vulnerabilities which may have been identified since the previous inspection.
 9. All firewalls shall log traffic on either a session (stateful) or packet basis. At a minimum, source and destination addresses and ports shall be captured along with relevant time stamps and action taken by firewall.
 10. Whenever possible, log information shall be replicated off the firewall platform. Firewall logs shall be retained in accordance with applicable information retention guidelines.

11. Identification, authentication and access rights to log data shall be controlled as the log data may be required for evidentiary purposes and chain of custody shall be demonstrable.

9.2 Remote Access

Remote access is defined as a temporary connection from a user to an NG9-1-1 network from another location. Examples of remote access include, but are not limited to the following examples:

- Remote connection to the NG9-1-1 network for maintenance purposes
- Remote connection the NG9-1-1 network in order to use an application specifically designed for remote use (i.e. mobile call taking software)
- NG9-1-1 users remotely connecting into the NG9-1-1 network for management or administrative purposes.

No remote access shall be permitted to any NG9-1-1 network unless addressed by contract, employee policy or similar legal instrument which contains adequate security language as determined by a security professional.

9.2.1 Client Based VPN and Consolidated Modem Pool

All client based VPN and/or consolidated modem pools shall be operated by the NG9-1-1 security organization or personnel contracted for that purpose as they enable access from public networks such as the PSTN or Internet. Strict controls shall be maintained for VPN and/or consolidated modem infrastructures as they enable access to the NG9-1-1 Entity from public networks such as the Internet or public switched telephone network.

All client based VPNs shall utilize industry standard technologies which preserve data integrity and privacy while in flight. Examples of such technologies are IPSEC and SSL based VPN. Some tunneling protocols, while sound networking technologies, do not provide mathematical assurances of integrity and privacy, such as PPTP and L2TP.

All client VPN and centralized modem pool access shall utilize strong authentication which includes single use passwords.

All client VPN and centralized modem pool access shall be controlled by a firewall. Such firewall shall be able to utilize the user's authenticated identity to impose access controls for that user and/or class of users (role based firewall policy).

All such access shall be logged. The log shall consist of authenticated identity, failed authentication attempts, time of attempted access, assigned IP addresses, time and date stamps, duration of access and internal locations accessed.

9.2.2 Directly Attached Modems

Use of modems which are directly attached to servers, routers, switches or other such equipment is strongly discouraged and generally prohibited by default in security best practice. However, certain conditions can be present which require their use. If needed, the usage shall be pre-approved, registered, documented and tracked in accordance with an exception process as documented in Section 12. Use of only “secured modems” shall be permitted. Uncontrolled use of modems can result in serious vulnerabilities and shall use risk mitigation measures.

When such modems are utilized through approved exception, they shall meet all criteria established for client based VPN or consolidated modem pools, including firewall access controls and single use passwords.

Directly attached modems shall use a third party authentication schema based on industry standards such as TACACS or RADIUS.

An accurate inventory of directly attached modems shall be maintained.

Other modem technologies which shall be considered include “dial/dial back”, active only when primary access means is down or attached only to devices which have strong authentication mechanisms.

9.3 Extranet and External WAN Connectivity

External connectivity is often required to meet communication requirements for vendors and information sharing or other such purposes. Appropriate measures need to be taken to mitigate risks and exposures which may be introduced by such connectivity. Further, since these connections often leverage public transport media, information should be protected in flight, particularly if dedicated facilities are not utilized.

9.3.1 Private Lines and Dedicated Layer 2 Virtual Networks

Private facilities can be utilized and often provide a reasonable assurance of privacy such as point to point circuits (T1, fractional T1, DS-3, SONET rings, etc). Also lower layer partitions such as DLCI interconnection via Frame Relay and or VPNs via MPLS can provide reasonable assurances of privacy. Such communication facilities generally provide a high degree of reliability and use of multiple connections with different physical paths can provide even higher availability for critical communications. When possible the aforementioned network technologies should be considered in lieu of communication over public transport. Use of these network technologies does not necessarily preclude the need for end to end encryption. Organizations should evaluate the importance of the data traversing the network and determine if encryption is appropriate to meet the necessary privacy levels.

9.3.2 Private Communication over the Internet

Communication via the Internet has the potential to be intercepted and retained using trivial technologies such as network protocol analyzers and sniffers. As a result, the Internet does not offer any assurance of privacy. Unless measures are taken to protect the data in flight such as

site to site or point to point VPN, any information transmitted via the Internet may be publicly or privately disclosed. Further, the identity of end points on the Internet cannot be determined with confidence.

However, these issues are well documented and a robust means exists to assure privacy of communication and the integrity of end points. Such solutions make use of tunneling protocols such as IPSEC and SSL. When communicating over public transport like the Internet communications shall be encrypted using IPSEC or SSL. When using such protocols, endpoint authentication shall be implemented using either certificates or similar credentials. Industry standard protocols shall be utilized and minimum key length shall be 128 bit.

9.3.3 External WAN Gateways

Since the external connection shall clearly be identified as an untrusted connection, a firewall shall be utilized to control the communication between the external endpoint or network and the internal NG9-1-1 environment. The firewall shall be implemented in a manner consistent with Section 9.1.

9.3.4 Demilitarized Zones (DMZs)

Certain applications (i.e. Web Servers, or email Bridgehead servers) may require access from external, public transport networks (i.e. Internet). These applications are commonly placed on special, external network segments commonly referred to as Demilitarized Zones (DMZs).

The DMZ provides intermediate environment for interaction with external domains without permitting access to internal domains or networks. This layering technique can improve the security posture of a system which requires an application to face the Internet without exposing the internal network.

When applications require access from external, public transport networks (i.e. Internet) they shall be placed on a DMZ, or shall be employ network based encryption and authentication mechanisms (i.e. VPN).

9.4 Intrusion Detection / Prevention

Use of network or host based intrusion detection or prevention technologies should be considered at network boundaries and/or on desired hosts. If used, they shall also be positioned on internal networks at strategic locations which may include high value networks such as those supporting call taking positions.

Intrusion detection/prevention signatures shall be routinely updated. Processes shall include well defined schedules for signature updates and shall include emergency update protocols for signatures required to detect high risk and day zero response events.

Intrusion Prevention technologies should be carefully deployed and implemented due to their automated response capability. False positive “hits” and related responses can result in interruption of legitimate traffic due to the automated responses. Careful design and configuration of intrusion prevention devices can help control these risks but not eliminate them.

It is recommended that Intrusion prevention technologies be implemented and managed by a security professional.

9.5 Layer 2 Security and Separation

Current network technologies permit different networks to share the same Layer 1 or physical facilities. Often these networks are called logical networks or multiple logical networks. This can include virtual router capability or VPN overlays over MPLS for virtual WANs or local LAN partitioning using VLAN or VRF technologies.

When such technologies are used, each VLAN, VRF or VPN shall be classified as required in Section 9.3. Once classified, these logical networks shall be treated as though they are different physical networks. All guidelines for use of firewalls, intrusion detection, remote access and all other relevant security principles shall be followed when designing interaction between virtual networks.

The equipment supporting virtual or logical networks can pose a unique risk. The routers and switches supporting these networks can be utilized as “islands” to hop between networks of different security classification. These risks can be managed using appropriate safeguards which may include the following:

1. All equipment supporting virtual or logical networks shall have a “management” tunnel for support and monitoring of the device.
2. Such equipment shall limit user group (write, read only, etc) access to particular virtual facilities whenever possible.
3. Commands (like telnet) which enable direct access between virtual facilities (sometimes known as “island hopping”) on the routers and switches shall be disabled or only allowed to be executed by the highest administrative privilege supported by the device. Such commands are typically vendor specific.
4. User access to devices supporting multiple virtual networks should utilize an industry standard authentication and access control protocol such as TACACS or RADIUS.
5. Layer 3 interactions between networks of differing security classifications shall only be done using a firewall or similar device

9.6 Network Redundancy and Diversity

9.6.1 Redundancy Considerations for On-Site/Local High Availability (HA)

Network redundancy is the duplication of equipment at a given site It can also include duplication of circuitry within a device such as control boards, power supplies, etc. Adequate redundancy can help avoid outages based on single hardware failure events. Typically protocols such as Virtual Routing Redundancy Protocol or Hot Standby Router Protocol are used to provide automated transfer of traffic between banks of equipment during failure events.

Traditional local HA in IP space can be handled by multiple elements:

1. Fast-action STP/RSTP/PVST+ re-converging redundant LAN switches or stacked LAN switches
2. Teamed NICs in servers and mission-critical desktop computers
3. If possible, redundant servers
4. HA firewalls
5. Redundant routers
6. Redundant WAN links
7. Out-of-band (OOB) communication links
8. Redundant premise wiring
9. Separate power feeds
10. Alternatives to commercial power.

Network redundancy can be difficult and expensive to design and implement, however, it is warranted when a very high degree of availability is required by the NG9-1-1 Entity. Network redundancy should be considered when implementing NG9-1-1 networks.

9.6.2 Diversity Considerations

Network diversity requires use of physically separate routing and cabling to provide further protection against outages triggered by a single event. Network diversity is more difficult and expensive to design and implement, however, it is warranted when a very high degree of availability is required by the NG9-1-1 Entity. The amount and nature of physical separation shall be clearly understood and defined for each location. Such separation may range from simple measures such as dual cable entrances on opposite sides of a given building to far more complex solutions such as different data centers in different cities. Routing protocols such as RIPv2, BGP and/or OSPF are used to perform automated transfer of traffic and/or service between physical locations.

Use of redundancy and/or diversity can have an effect on various types of security products. Most notably, traffic failover between different cities and different firewall sites can result in dropping sessions which are underway at the time of the failover. Applications shall be designed to elegantly recover such events and users advised as to proper “restart” procedures in case such a failover event was to materialize.

Network diversity should be considered when implementing NG9-1-1 networks.

10 Change Control and Documentation

Changes to the architecture, design or engineering of the NG9-1-1 networks shall include a formalized pre-cutover and post-cutover security review by the Local or Regional 911 security representative of NG9-1-1 Entity and any 3rd party vendors. A formal change control process shall be followed and appropriate documentation shall be produced and retained. If the change is complex, for example:

1. Connecting to a new untrusted/unknown network.
2. A new transport mechanism is used

3. A new authentication, authorization, accounting, or auditing framework is used
4. A new management ENTITY is used
5. A new IP allocation scheme is used
6. A new routing arrangement is used
7. A new security perimeter is redrawn

A team of Subject Matter Experts (SME) shall be assembled to review and approve the change.

11 Compliance Audits & Reviews

NG9-1-1 networks can be deployed in a number of different manners including; local, regional, national or even global. It is anticipated that initially local and regional NG9-1-1 networks will be deployed, and that the responsible agencies will develop appropriate policies (including security policies) for those systems. As national and/or global NG9-1-1 networks are deployed, it may become necessary to create organization(s) responsible for compliance auditing.

In the meantime, the agencies that deploy **NG9-1-1 networks** and develop security policies for them are required to conduct periodic audits or reviews to ensure that both the **NG9-1-1 networks** and the systems that are connecting to it comply with the security requirements listed in this NENA standard.

Audits can be conducted internally or externally. Internal audits are used to "self-check" an organization's compliance with security standards and/or policies. An external audit leverages a non-biased 3rd Party to independently perform the audit. Both methods are valid and useful.

- Internal Audits shall be conducted at a minimum of annually.
- External audits shall be conducted at a minimum of once every 3 years.
- Security audits shall utilize various methods to assess the security of networks and processes, applications, services and platforms including automated tools, checklists, documentation review, penetration testing and interviews.
- Findings resulting from such security assessments shall be subject to corrective actions. Such corrective actions shall be applied to the satisfaction of the organization managing the security assessments

NG9-1-1 Entities performing internal audits or "self-checks" may use external, 3rd party resources if necessary.

Findings resulting from such security assessments shall be subject to corrective actions. Such corrective actions shall be applied to the satisfaction of the organization managing the security assessments.

12 Exception Approval and Risk Acceptance Process

As the responsible agencies choose to adopt the security, requirements, and guidelines listed in this standard, there may be occasions when it is not possible to comply due to technical constraints, cost restrictions, or other reasons.

When such occasions arise, the resultant security risk shall be identified, documented and managed in accordance with the guidelines given below. **Be aware the non-compliance can put NG9-1-1 networks at risk. By signing an Exception Approval/Risk Acceptance Form, the NG9-1-1 Risk Acceptance Approver acknowledges that risk and that acceptance may absolve its service provider of any financial and liability responsibilities. Exception Approval / Risk Acceptance Forms should be included as a part of contracts or agreements if applicable.** It is highly recommended the NG9-1-1 Security Risk Manager and the Security Point of Contact get their legal and security organization involved when they have questions.

The exception approval and risk acceptance process shall consist of five phases:

1. **Risk justification:** Provides a business case for waiver or exception of the security requirement
2. **Risk identification:** Aims to thoroughly and unambiguously define the risk, the scope of what is at risk, and how the risk was identified.
3. **Risk assessment:** Uses three risk factors to assess: the potential severity of the risk, the impact of the risk, and the likelihood of the risk actually happening. These factors assist in deciding the mitigation of the risk, and in determining the frequency of review for the risk.
4. **Risk analysis:** Evaluates the feasibility and costs of different mitigation strategies relative to the potential cost impact.
5. **Risk acceptance and approval:** Only when risk cannot be totally removed or reduced to an acceptable level then it has to be accepted as is and get approval from NG9-1-1 Risk Acceptance Approver and include an Exception Approval/Risk Acceptance Form (EA/RAF).

All of the above shall be documented on the EA/RAF, including the names and contact information of the people who carried out the analysis.

12.1 Exception Approval and Risk Acceptance Process Scope

The exception approval and risk acceptance process shall be followed for *all risks* (e.g., security vulnerabilities cannot be fixed or security patch cannot be applied, cases of non-compliance with this Security Standard).

The specific non-compliance or vulnerabilities documented in the EA/RAF shall be reviewed by NG9-1-1 Entity security organization and legal department. The actual form shall be maintained and tracked by the NG9-1-1 Entity Security Risk Manager, the Security Point of Contact (Security POC), and all involved parties.

Exceptions based on legal or regulatory requirements shall still be documented by EA/RAF form for tracking purposes.

12.2 Roles and Responsibilities in the Exception Approval and Risk Acceptance Process

The capture, assessment and management of a risk require the involvement of a number of individuals / teams who are required to fulfill certain roles. While others may be involved, there are three specific roles:

12.2.1 NG9-1-1 Security Risk Manager/Applicant

NG9-1-1 Entity shall assign a Security Risk Manager to manage security risk for NG9-1-1 network and who shall be responsible for completing the EA/RAF in a complete and accurate manner prior to submitting it to the appropriate Security Point of Contact / Team for review. The Security Risk Manager shall collaborate with other members of the pertinent security team in completing the form. The Security Risk Manager shall also obtain the approval signature from the NG9-1-1 Entity Risk Acceptance Approver.

The person filling the role of NG9-1-1 Entity Security Risk Manager/Applicant shall be an employee or an authorized agent acting on behalf of the NG9-1-1 Entity and may be determined in several ways. The Security Risk Manager may be, but not limited to, any one of the following:

1. The person identifying the need for execution of the exception approval and risk acceptance process with technical and business knowledge of the asset(s) at risk.
2. A system administrator, systems engineer, project manager or other key stakeholder with technical and business knowledge of the asset(s) at risk.

The NG9-1-1 Entity Security Risk Manager shall act as the point of contact for the organization owning the identified asset(s) at risk within the scope of the exception approval and risk acceptance process for the active duration of the EA/RAF. If the Security Risk Manager leaves the NG9-1-1 Entity or changes job responsibilities during the active duration of the EA/RAF, a new Security Risk Manager shall be identified to fill the role.

12.2.2 Security Point of Contact / Team

The Security Point of Contact / Team shall be responsible for reviewing the EA/RAF for completeness, accuracy and consistency given their experience and subject matter expertise. For high level risks, a team of Subject Matter Experts (SME) shall be assembled to review the EA/RAF and sign and document their concurrence position on EA/RAF prior to submission for NG9-1-1 Entity Risk Acceptance Approver's approval.

12.2.3 NG9-1-1 Risk Acceptance Approver

The senior manager (e.g., NG9-1-1 Entity Operation Manager or Director) within the NG9-1-1 Entity shall be responsible for signing to accept complete accountability for any identified risk. Responsibility for approvals shall not be delegated to subordinates or peers, and shall adhere to the management levels specified or higher. Generally, the appropriate senior manager for accepting the risk and approving the exception has financial and legal responsibilities for the services and operation of the specific NG9-1-1 Entity.

In cases where the assets at risk are not limited to a single device/application/network at one NG9-1-1 Entity location (e.g., it can potentially spread to associated NG9-1-1 Entity locations or other network domains), the EA/RAF reviewing Security POC / Security Teams may determine that the exception approval and risk acceptance shall be obtained from more than one senior managers. Assets that support multiple services may, as determined by the reviewing Security POC / Security Team, require concurrence from the Operations and Engineering senior management accountable for the availability and operability of the assets.

12.3 Process

Risks to NG9-1-1 are extremely important and they shall be acknowledged, assessed and managed according to their severity.

12.3.1 Process Flow

1. The NG9-1-1 Entity's Security Risk Manager identifies, justifies, assesses, and analyzes the risk. If the identification and/or analysis of the risk prove to be difficult, then a security team shall be contacted for assistance. The Security Risk Manager shall complete the EA/RAF, including Risk Justification, identifying the Security POC / Team, and NG9-1-1 Entity Risk Acceptance Approver.
2. The Security Point of Contact / Team shall assign the EA/RAF a globally unique tracking identifier / document number, review the form, determine or agree to who the NG9-1-1 Entity senior management approver is, discuss with Security Risk Manager until agreement reached or no more progress possible, involve a team of SMEs as necessary.
3. NG9-1-1 Entity Security Risk Manager signs EA/RAF.
4. The Security POC / Team documents concurrence position and signs the form
5. NG9-1-1 Entity Risk Acceptance Approver (senior manager) reviews the form, determines/documents strategy and reason, ensures risk mitigation is completed on the form, and accepts full responsibility and accountability by signing the EA/RAF.
6. The Security Risk Manager shall ensure the completed EA/RAF along with all necessary signatures/approvals, either physical or electronic, are filed with the reviewing Security POC / Team.
7. The Security Risk Manager, Security POC / Team, and Risk Acceptance Approver as well as other involved parties shall separately retain the form, either physical or electronic, for their records.

Risks being reviewed / renewed, i.e., not new, shall be thoroughly reviewed by the Security Risk Manager and reassessed by Security POC / Team prior to submitting to Risk Acceptance Approver/senior management to ensure that the information is current.

12.3.2 Tracking and Documentation

The required level of tracking/documentation is dependent on the time period in which the risk can be eliminated. See table below:

Risk Category / Severity	Time to Eliminate Risk	Risk Exists Less Than the Specified Timeframe and Minimum Required Level of Tracking	Risk Exists More Than the Specified Timeframe and Minimum Required Level of Tracking
Critical	Immediate action is required	Escalate until resolved	Escalate until resolved
High	30 days	Security POC / Team and all involved parties shall be kept informed of progress and Risk Acceptance Approver to be made aware by Security POC / Team	Full Documentation and Approval
Medium	60 days	Security POC / Team and all involved parties shall be kept informed of progress	Full Documentation and Approval
Low	90 days	Security POC / Team and all involved parties shall be kept informed of progress	Full Documentation and Approval

NOTE 1: During a virus outbreak, such as Code Red, Blaster, or Slammer worms, as soon as the NG9-1-1 Entity Security Risk Manager, Security POC / Team, or authorized agent acting on behalf of an NG9-1-1 Entity receives a **critical** level alert from a centralized Security Advisory authority, action shall be taken immediately to address the risk. **A critical risk may require implementation of emergency measures.** These measures may include applying patches immediately and preparing to operate the NG9-1-1 Entity in a diminished mode.

NOTE 2: Once the risk category for a particular security risk is assessed, that risk level shall not be changed unless sufficient evidence is identified or there is justification for the change. All involved parties shall agree to the risk re-assessment before the start of the same exception approval and risk acceptance procedure. Risk category shall not be downgraded simply because it cannot be eliminated or reduced by the specified timeframe.

12.4 Review Period

All documented risks shall be periodically reassessed according to the associated risk category, and specified timeframes in the table below. If not then the EA/RAF expires leading to a state of non-compliance.

Risk Category	Review Period (months)
Critical	0
High	3
Medium	6
Low	12

Review period to be based upon the date associated with the first signature/approval of EA/RAF. Evidence of the approver's periodic reviews and continued approval and acceptance of risks shall be documented and submitted to the appropriate Security POC / Team then distributed to all involved parties. The EA/RAF shall be stored according to NG9-1-1 Entity and involved parties' record retention policy.

When a risk comes up for renewal, and a previously documented compliance action was not completed, the senior manager required for signature of the renewal shall be escalated to at least one level higher than before.

12.5 Change of Circumstance

Any change to the circumstances identified in the EA/RAF that will affect the associated risk, shall immediately be clearly documented in a revised EA/RAF, submitted to the appropriate Security POC / Team for review, and presented to the appropriate NG9-1-1 Entity Risk Acceptance Approver / senior manager for review and re-approval. Re-approval shall adhere to the same procedural formality as initial acceptance and approval.

12.6 Risk Identification

To ensure the capture of all relevant information in clear and meaningful terms, the identification of a risk can be divided in to a number of sub areas.

12.6.1 How was the Risk Identified?

There are various ways that network and computing security risks can be identified. For example:

1. A centralized Security Advisory authority (e.g., a NG9-1-1 Entity consortium staffed by their own security personnel or a service provided by a third party), report generated from local host IDS tool or local/remote vulnerability scan tool
2. Security compliance reviews, assessments, or audits: Security assessment of new or changed technology including product limitation, pre-production, post-production security review/assessment, security review program, new network connection/interface submissions, contract reviews, outsourced projects, ad hoc

discovery by the security organization, proposed new services, or non-standard customer requirement.

12.6.2 What is At Risk?

Some or all of the following will be required to fully describe the nature of what is at risk:

1. Service name(s), e.g., VoIP, MPLS/VPN, premise device management service, security management service, third party service
2. System process associated to the resources at risk, e.g., system change process, system patching process
3. Internal, commercial or outsourced service
4. Contract periods involved
5. Number of systems affected
6. Database system, middleware, application language, application name(s)
7. Number of users affected
8. Type of users affected, e.g., call taking position user, system administrator
9. Type of device, e.g., router, switch, workstation, server
10. Operating system(s), e.g., Windows 2000
11. Where are they physically located
12. What network(s) are they connected to, e.g., LAN, WAN

NOTE: It is important to consider not only what is placed at PRIMARY risk, that is the system(s), service(s), etc. directly at risk, but to also consider what if any system(s), service(s), etc. are at SECONDARY risk.

FOR EXAMPLE: When the risk under consideration relates to system(s) solely in support of a given NG9-1-1 Entity, e.g., a CPE firewall, it is essential that the risk analysis takes into account any risk to other NG9-1-1 Entity systems or services provided by others.

It needs to be clearly described exactly what is at risk, and the scope of assets at risk, e.g., class A versus class C IP address ranges, all systems on NG9-1-1 Entity's LAN versus just a single server in DMZ. In cases where the risk(s) are identified to span multiple assets, e.g., secondary systems, networks, multiple NG9-1-1 Entity's Risk Acceptance Approver / senior managers shall be required to approve the EA/RAF and accept accountability for the risk(s).

The version and section number(s) of non-compliance in the Security Guidelines document shall be fully defined in the EA/RAF. Along with details of the nature of the risk, the threat posed circumstances and the deviation from the Security Guidelines.

Attach all appropriate technical documentation, e.g., architectural diagrams or system descriptions, to support the risk identification and mitigation strategy.

12.6.3 Risk Assessment

In order to aid the consistent analysis of risk, and facilitate the comparison of the security risks a formal risk assessment model shall be used. This model derives a risk category from three (3) associated risk factors:

1. Vulnerability (in terms of both current and future contexts), i.e., what is the severity of the risk
2. Impact, i.e., what would it mean to NG9-1-1 Entity if the vulnerability were exploited, and
3. Threat, i.e., what is the likelihood of such an exploitation

NOTE: During a virus outbreak, such as Code Red, Blaster, or Slammer worms, as soon as the NG9-1-1 Entity Security Risk Manager, Security POC / Team, or authorized agent acting on behalf of an NG9-1-1 Entity receives a **critical** level alert from a centralized Security Advisory authority, action shall be taken immediately to address the risk. **A critical risk may require implementation of emergency measures.** These measures may include applying patches immediately and preparing to operate the NG9-1-1 Entity in a diminished mode.

Also, during this time further risk assessment, analysis, and documentation may have to be delayed until the critical risk is resolved or mitigated.

Having assessed each of the three (3) risk factors in turn so as to assign them individual categories of: High, Medium or Low, they are then combined to obtain the overall risk assessment category:

1. High
2. Medium
3. Low

12.6.4 Vulnerability Assessment

Vulnerability assessment involves quantifying the severity of the risk being considered. Data to help in this assessment may come from using a security assessment tool (e.g., a vulnerability scanning tool, a local host IDS tool), having a security audit done by an authorized security company/organization, or security review by security SMEs.

In the event where more than one "What can be done" scenario exists, multiple vulnerability assessments (High, Medium, or Low) may be assigned. The highest rating takes priority.

Use the example table below to determine the vulnerability rating:

What can be done?	What type of User ID / access is required?	Vulnerability Assessment
Unauthorized access or improperly controlled	None	High

access through a filtering device.	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to an Administrative User ID.	None	High
	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to a Call Taking Position User ID.	None	High
	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to NG9-1-1 Sensitive (Restricted) or NG9-1-1 Sensitive (Most Sensitive Information) data.	None	High
	General	Medium
	Administrative	Low
Unauthorized access or improperly controlled access to NG9-1-1 Sensitive (Internal Use Only) data.	None	Medium
	General	Low
	Administrative	-Not Applicable -
Denial of service attack affecting call taking position users or services those are not local to the device under attack.	None	High
	General	Medium
	Administrative	Low
Denial of service attack affecting only call taking position users or services that are local to the device under attack.	None	Medium
	General	Low
	Administrative	-Not Applicable -

In the example table above the following definitions are assumed:

1. Filtering device includes: Routers, firewalls, other network components and operating systems capable of restricting access through that device by means of filters, access control lists, etc. For example: Cisco router ACL, Checkpoint Firewall-1 rule set.
2. Administrative User ID: Any User ID having either system administrative, or security administrative authority. For example: UNIX root, Windows Administrator.
3. General User ID: Any User ID not falling into the "Administrative User ID" category.
4. NG9-1-1 Proprietary Data (Restricted or Most Sensitive Information)
5. NG9-1-1 Proprietary Data (Internal User Only)

Where the above example table does not allow a reasonable assessment of the risk being considered, the NG9-1-1 Entity's Security Risk Manager shall select a vulnerability assessment and document the justification for that selection.

NOTE: The above example table shall be used to assess what can be achieved rather than how it is achieved. So for example: If arbitrary code can be executed to gain UNIX root or Windows Administrator access, then it is the ability to gain root or administrator access that is important rather than that it was obtained by executing arbitrary code.

When documenting the reason for the vulnerability rating assigned include information about the purpose and capabilities of the assets, associated applications, current users and available access, trust relationships that could allow propagation, and any other information to provide full disclosure of the risk.

12.6.5 Impact Assessment

The impact assessment shall consider both direct and indirect impacts when determining the inventory of assets that could be affected. For example: A direct impact of a vulnerability when exploited may be unauthorized access to a given system and disclosure of information.

However, an indirect impact may result if the unauthorized access can be used to gain further access to other systems in a networked environment.

When conducting an impact assessment, areas of impact should be analyzed using qualitative (e.g. loss of life, front page of the newspaper, etc) and quantitative means (e.g. financial loss, down time, etc).

12.6.6 Threat Assessment

Threat assessment involves quantifying the likelihood of the risk under consideration becoming a reality, that is, of it being exploited. Threat is actually a combination of two sub factors:

1. Capability, i.e., how able to carry out the attack are the attacker(s) likely to be. This will depend on the nature of risk and involves quantifying the sophistication and availability of hardware, software, skill, and knowledge necessary to exploit a given vulnerability. The threat assessment category shall also take into account any existing mitigation strategies in use that could lessen the threat, e.g., strong/one-time authentication, filters, etc.
2. Intent, i.e., how determined the attacker(s) are likely to be. This will depend upon the motivation of the attacker(s) and what benefits, e.g., financial, intellectual, revenge, that they think they will obtain.

NOTE: A state of full intent is always assumed, therefore, threat becomes capability.

The threat assessment of High, Medium or Low for a risk is determined as the most severe category for which any one criterion is satisfied. When documenting the reason for the threat rating assigned describe the sophistication and availability of hardware, software, skill, and knowledge necessary to exploit a given vulnerability. Identify all factors considered that could increase or decrease the ease of exploitation.

12.6.7 Determining the Risk Assessment Category

Risk Assessment involves the comparative assessment of available options. Documentation shall clearly articulate the possible corrective actions, their cost in time and resources to implement, their effectiveness for reducing or eliminating the risk, the residual risk that will remain, and the reduction in impact from exploitation that will result from each different option. Such that the

NG9-1-1 Risk Acceptance Approver / senior manager will be able to make a business decision based upon these facts.

The possible responses can be broadly grouped into four categories:

- Risk elimination
- Risk reduction
- Risk acceptance
- Risk transfer.

The information documented relating to each possible response shall be sufficient to ensure accurate costing, assessment and costing of residual risk, time to implement, possible constraints, and any other pertinent details. Regulatory requirements, technological issues, or performance implications may affect the decision to implement, or not implement, security measures. It is necessary to understand these constraints and document them in order to formulate and support the appropriate mitigation strategy.

12.6.7.1 Risk Elimination

From a purely security standpoint this is the preferred approach; however, even when this is supported by the business decision it shall be understood that it will take time to attain. The commitment for any expenditure or resource allocation that is necessary, and the planned date by which the risk will be eliminated shall be documented.

12.6.7.2 Risk Reduction / Mitigation

Risk reduction / mitigation can take various forms. Some of the options that shall be considered:

1. Contractual: For example, Non Disclosure Agreement (NDA), addition of stringent security requirements and audit rights
2. Physical: For example, enclosure of equipment within a locked cage, purchase additional hardware to separate computing environments
3. Logical: For example, add filters to restrict access (e.g., source IP address, protocol, application, SNMP MIB (Management Information Base) for Windows) implement or strengthen authentication (e.g., tokens, digital certificates), implement or strength authorization (e.g., read-only permissions, group restrictions)
4. Procedural: For example, call Network Operations Helpdesk before and after doing "X", add notification process when certain account access has been changed

As previously stated the implementation costs, timings and residual risks need to be considered for each option. Any mitigating controls that are in place shall be documented, along with the commitment for any expenditure or resource allocation that is necessary, and the planned date by which the risk will be reduced to the agreed upon level.

12.6.7.3 Risk Acceptance

The option of doing nothing to reduce the level of risk is not encouraged, but may in certain circumstances be appropriate owing to technical limitations, or prevailing business

circumstances. **Any such acceptance of risk by NG9-1-1 customers shall be clearly documented in applicable contractual agreements.**

For the case where risk acceptance is used then residual risk rating will be as initially assessed and the potential impact cost should the risk occur would be as seen in the Section 12.6.5 Impact Assessment. Any mitigating controls that are in place shall be documented.

12.6.7.4 Risk Transfer

Risk transfer is generally covered under the state, local, or federal statute where applicable.

12.6.8 Fields on Exception Approval and Risk Acceptance Form

The following are the recommended sections and their associated fields to be included on the form.

1. Security Risk Manager – Detailed contact information
2. Risk Justification – a business case justifying the risk
3. Risk Identification – Description of risk (refer to Section 12.6 for detail) and date the risk was Identified
4. Risk Assessment – Rating (high, medium, low) for each assessment and the reason the particular rating is obtained
 - a. Vulnerability
 - b. Impact
 - c. Threat
 - d. Overall Risk Assessment rating (high, medium, low) is derived from the vulnerability, impact, and threat assessments.
5. Risk Analysis – Document the comparison between the cost of eliminating the risk with the cost of it becoming a reality (refer to Section 12.6 for detail)
6. Risk Mitigation – Document what strategy will be used, how, why, and when is it expected to last until. The exact approach (e.g., elimination, reduction, or acceptance) shall be clearly specified in this section.
7. Review Period – Based on the risk category (high, medium, low), re-review period of 3, 6, or 12 months will be assigned. Document the exact expiration date (from the date of the first signature on this form). **Make sure all parties involved are aware the re-approval shall adhere to the same procedural formality as initial exception approval and risk acceptance. Failure to review would lead to a state of non-compliance.**
8. Signatures – Sign to certify that this is an accurate assessment of the identified risk
 - a. NG9-1-1 Security Risk Manager – Include name, NG9-1-1 job title, organization, and date.
 - a. Security Point of Contact (Security POC) / Team – Sign to certify concurrence that this is an accurate assessment of the identified risk only after the Security Risk Manager has signed. Include name, job title or organization name, date, conditional concurrence or non-concurrence, and any comments.

- b. NG9-1-1 Risk Acceptance Approver (or senior manager) – Sign to acknowledge approval of the identified risk only after the Security Risk Manager and Security POC/ Team have signed. By signing this form, this approver is **accepting complete accountability** for the identified risk and **commitment** to the plan as defined in the Risk Mitigation section. Include name, job title, and date.

See Appendix 4 for a sample risk acceptance and approval form.

NOTE: The Exception Approval and Risk Acceptance Form is an auditable record and copies must be retained by all signatories and affected parties for at least one year or longer according to regulatory requirements from closure of risk.

13 Incident Response & Planning

An Incident Response Plan shall be implemented. An Incident Response plan is defined as:

The formal, written plan detailing how an organization will respond to a computer security incident. Examples of security incidents include virus outbreaks, hacking attempts, critical service outages, denials of service, and more.

Responding to security incidents is an important part of an effective IT Security program. In order to rapidly detect incidents so as to minimize loss and destruction as well as restore service an incident response plan is necessary. Appendix 1 (Section 14.1) provides best practices and recommendations regarding the creation and execution of Incident Response Plans.

13.1 Appendix 1: Incident Response Planning

13.1.1 Incident Response & Planning

Responding to security incidents is an important part of an effective IT Security program. In order to rapidly detect incidents so as to minimize loss and destruction as well as restore service an incident response plan is necessary. An Incident Response plan is defined as:

The formal, written plan detailing how an organization will respond to a computer security incident.

Examples of security incidents include virus outbreaks, hacking attempts, critical service outages, denials of service, and more

This section is intended to provide personnel with the suggested procedures for identifying, reporting, and responding to computer and network security incidents.

This is applicable to:

- All personnel that perform functions or services that require securing information and computing assets.
- All devices and network services that are owned or managed by the service provider, vendor or NG9-1-1 Entity.

13.1.2 Background

Identification and reporting of computer and network security incidents shall be required to:

- Contain the incident and minimize the loss or compromise of information assets.
- Enable the initiation of the appropriate legal process.
- Correlate activity with other incidents to allow for coordinated action and to prevent duplicated efforts.
- Gather statistics for identifying trends and development of security measures to counteract vulnerabilities.
- Improve procedures and guidelines.
- Handle requests for security related information.

NOTE: All personnel shall notify the identified incident response service provider if any computer, computer system or network is compromised or if a breach of security is suspected or is in progress that involves internal network(s) and commercial network(s) owned and/or managed by service provider, vendor or NG9-1-1 Entity. It is important to note that regardless of the location where the suspected incident occurs or is observed, the identified incident response team shall first be notified. Security Point of Contact / Team will confirm the violation or make a record of it as appropriate and coordinate all further investigative and recovery efforts.

13.1.3 Roles and Responsibilities

A security agent shall be responsible for managing all investigative activities related to computer and network security incidents, and for managing the intrusion response effort. Investigative activities include, but are not limited to:

- Maintaining a list of SMEs, including name, department, contact information and areas of expertise.
- Contacting appropriate team members as needed in response to an intrusion.
- Coordinating intrusion response efforts,
- Interviewing witnesses,
- Reporting to management regarding an intrusion and response,
- Coordinating efforts with other organizations and other companies.
- Diagnose the event with the assistance of the local system administrator and determine the course of action to be taken.

13.1.3.1 Incident Reporting/Response Notification Contact Details

Any suspicious or unusual activity, which may indicate an attempt to breach the integrity of Public Safety's networks and systems, shall be reported immediately to an established Security Incident Response Team or equivalent. Any, and all, actual, attempted, and/or suspected misuse of Public Safety assets shall be reported immediately to the appropriate organizations.

All personnel shall be required to report all incidents to IR Service provider by one of the following methods:

- Hotline
- Website
- Email
- In Writing

All personnel shall use discretion when communicating suspicious activity, for example - do not send information about the attack via email if you suspect the computer or communication channel has been compromised. All personnel shall utilize the hotline to notify when online mechanisms are questionable, or the incident is of an urgent nature.

13.1.3.2 Intrusion Response Team

Responsibilities of the SME group assembled include, but are not limited to:

- Gathering and preserving evidence as it relates to intrusions,
- Providing evidence and evidence analysis to the security department, and
- Recommending changes to prevent and protect against future intrusions.

13.1.3.3 Asset Protection

Once the event is associated to a particular process, employee, contractor, vendor or other external ENTITY or individual, the group who is responsible for asset protection shall assume the responsibility for completing the investigation with the consultation and cooperation of the Security POC / Team. All members of the investigating team shall be expected to document their actions thoroughly, retain a copy of their notes for future reference, and submit a copy to the group who is responsible for asset protection to continue the investigation. The asset protection group shall retain all records, notes and reports in accordance with company retention guidelines. Evidence shall be protected, documented, and preserved once it is identified and seized. Any event being reported to law enforcement, or inquires from law enforcement, shall be coordinated by the asset protection group, excluding the normal subpoena submission process.

13.1.3.4 Managers

Management shall be aware and supportive of the additional responsibilities that their staff may have in association with the response effort.

13.1.3.5 Administrators

Administrators responsible for the day-to-day operations and/or security of information resources shall have the following responsibilities in connection with security intrusions:

- Confirming that an intrusion has occurred (or is occurring),
- Reporting the intrusion accordingly,
- Taking any immediate action as directed by Incident Response team,
- Keeping records of work efforts,
- Activating additional event logs,
- Where feasible, taking steps to prevent authorized entities from accessing the compromised system until evaluated.
- Cooperating in the investigation of the intrusion.

13.1.3.6 Detection and Response

If information resources are in danger of being irreparably harmed, the administrator shall take immediate action to protect these resources and implement the Business Continuity/Disaster Recovery (BC/DR) plan.

Examples of irreparable harm include, but are not limited to:

- An intruder has entered a system and is in the process of destroying or damaging data which cannot be recovered,
- An intruder is actively bringing systems down and impacting customer service, or
- An intruder is actively engaged in other behavior that will cause unrecoverable loss or damage to information resources.

Recommended actions include:

- Disabling all system accounts and/or changing all system passwords and /or disabling access permissions if allowed by the BC/DR plan,
- Correcting the vulnerability that allowed the intruder to gain access in the first place,
- Removing or shutting down the access method being used by the intruder,
- Bringing the system down or disconnecting it from the network, and
- Physically removing disk drives, tape files, or other system resources.

NOTE: If the NG9-1-1 Entity simply cannot shut the system down, then it shall go into a reduced production mode so the damage can be contained.

13.1.3.7 Information Disclosure

If a request for information is received, the appropriate security and legal organizations shall be contacted before responding. Personnel shall not disclose information about a security incident unless authorized by legal or Security Team.

Details relating to computer and network security incidents shall not be included in problem management records. Access to such details shall be controlled on a need to know basis.

NOTE: When proprietary information is inadvertently disclosed by Public Safety personnel, he/she shall immediately contact the Incident Response Team. The Incident Response Team shall contact Security Team if the information is security-related.

13.1.3.8 When to Contact the Incident Response/Reporting Team

The Incident Response/Reporting Team shall be contacted when:

- An active attack is detected.
- Activity which could be an attack is occurring.
- A suspected or actual security breach has occurred.

The following list of incidents is provided as examples only and is not considered comprehensive:

- Email related, such as: phishing, hoaxes, chain letters, hate mail, etc.
- Detection of Malicious code, such as: viruses, worms, Trojan horses, vulnerability exploits, etc.
- Web access related, such as: copyright violation, downloading prohibited files (music, video, etc.), etc.
- Intrusions – attempts (whether successful or failed) to gain unauthorized access to systems or data.
- Denial of service
- Inappropriate use of company equipment for processing or storage of data
- Compromise of system integrity or corruption of data – changes to system hardware, firmware or software without the owner’s knowledge, instruction or consent.

13.1.3.9 What Details to Report

Gather as much detail as possible to facilitate a timely and accurate assessment of the situation. Discussion of the situation shall be limited to those individuals with a direct need to know. The information outlined below is needed for incident response and investigation, it shall be provided if applicable:

NOTE: This is not an exhaustive list since each incident is unique.

- Point of contact for investigation.
- Originator of the incident, if this is not the same person as the contact person.
- Has this been reported before? Provide ticket number of previous reports or if reported to other organizations provide details.
- Is auditing turned on?
- If this involves customers provide details.
- Nature of the problem? Is the activity ongoing?
- Is there a backup of the affected system and is it available? (Not for use or disclosure outside NG9-1-1 Entity except under written agreement)
- What is the suspected business impact?
- What information has been exposed (Proprietary, etc.) and its classification if it is Proprietary in nature (This is important since suspected compromise of certain classifications of proprietary information could result in stringent individual notification processes involving privacy and legal involvement that would need to be initiated independent of this incident response process.)
- Identify the physical location of the assets involved.
- IP addresses and domain names of the machines involved (origination and destination).
- Network name to which the machine is connected.
- Date, time (including time zone), and duration of the activity.
- What is the suspected method of entry/origination?
- Operating system and patch level of systems involved.
- System clock time.
- System logs if available.

13.1.3.10 Next Steps

The Intrusion Response Team working with the appropriate Subject Matter Experts and representatives from other organizations shall perform the following steps:

- Discovery and report
- Incident confirmation
- Investigation and containment
- Recovery
- Post mortem and lessons learned

13.2 Appendix 2: Patching Best Results

The steps involved in applying security patches include:

1. Taking vulnerability advisories / security patch feed from various sources and/or (preferably) obtaining them from a consolidation service which performs vulnerability review and suggests priorities which can be a severity level and/or a target fixed duration, e.g., patch within 7 days
2. The devices' management authority receives notification of the patch or the vulnerability advisory and identifies the affected devices under his/her control.
3. Affected devices may be servers, desktops, Operating Systems, applications, middleware, network elements, and "black box" appliances which may have affected vulnerable components, e.g., application-specific call-processing equipment which uses Windows Operating System with .Net and SQL server.
4. A centralized security authority (which may be a NG9-1-1 Entity consortium owned security function or a service provided by a third party) assess the severity, risks involved, and production impact, then assigns the targeted fix duration
5. If a security vulnerability has a mitigation, please see #9 of the next section "General Patching Work Flow".
6. If a security vulnerability cannot be fixed or a security patch cannot be applied (e.g., equipment vendor/integrator unwilling to address the security issues, patch breaks the application, patch is incompatible with the other device components, patch cannot address the issues, patch has not been made available, no support on end of life equipment, system owner refuse to upgrade for any reasons, etc.) within the specified "targeted fix period" while there is no mitigation existing, an exception form shall be filled with the risk-acceptance ENTITY clearly identified.
7. Theoretically, full-time completely isolated NG9-1-1 Entity environment (as a quarantined "clean room") can be considered as a special case for exemption for few security deficiencies, such as not current in security patching practice. However, the defense of full time and completely isolated environment can hardly be maintained nor can be guaranteed, e.g., a service person brings in a laptop and connects to the supposing "isolated" local LAN or a person is plugging in a USB flash drive with unknown content into computer's USB slot. Accepting the risks of using the "isolated air gap" as the mitigation has to be performed by the NG9-1-1 Entity owner as a business risk acceptance.

13.2.1 General Patching Work Flow

At this point, security patch is just a class of different patches. The following is a sample flow on a generic patch process. Note that a patch can be a regular feature enhancement upgrade, bug fixes patch (e.g., a service pack), or a security patch.

1. Devices' management entities related to the patch category (OS, application, middleware, etc.) have to test/verify the patch. Patch shall be obtained from its original source (usually from the software publisher itself.) If a device's patch

- test/verification requires vendor/manufacture assistance, proper procedure shall be used. Test/verification task shall not be performed in production environment and shall not affect the production activities.
2. Very often a patch may have a potentially broader impact than just limited to itself (e.g., an OS patch may break the application), all affected parties have to approve the patch or sent-back for corrective actions, e.g., fix the patch itself.
 3. A "black box" appliance shall be patched and maintained by vendor responsible for such appliance. There is no special "exempt" status on such device.
 4. Once a patch is approved, it is scheduled to be applied over one or more maintenance windows.
 5. Patch shall be delivered to individual NG9-1-1 Entity using approved methods to ensure its integrity as well as to make sure the delivery channel/mechanism itself might not turn into a path of attack conduit or information leakage. Communication channel security is generally addressed within NG9-1-1 Entity networking architecture framework and the associated network security. The delivery mechanism may also include commercial couriers or hand-delivered. Content integrity can be assured by cryptographic checksum and digital signature.
 6. Depending on the potential impact of the patch a full backup on the system may be needed.
 7. Since NG9-1-1 Entity is a mission-critical environment, a rolling patching scheme or a phased patching scheme shall be pre-planned. It should be based on if the production tasks can be transitioned to or taken over by another device or function. If a single point of failure (SPOF) is identified, then alternative strategies as described in HA & BC/DR section shall be used.
 8. As a common practice, any patch shall have a back-out/recovery procedure created, tested/verified, and fully documented. In the case of fault or instability caused by the patch, the back-out/recovery procedure shall be used to roll-back the environment to the state prior to patching activity.

NOTE 1: Certain production data/user data may be irreversible and cannot be recovered.

NOTE 2: due to vendor's own product design, certain patches are not reversible. In such case, full restoration can be considered.

9. If an issue (including security vulnerability) cannot be fixed for various reasons (e.g., patch breaks the application, patch is incompatible with the other device components, patch cannot address the issues, patch has not been made available, no support on end of life equipment, etc.) and an equivalent and equally effective mitigation method is available, it may be considered as the last-resort solution. Such mitigation shall be treated on a per-case basis. Mitigation shall be fully documented, tracked by document change-control process and time-bound such that when there is a fix, the proper way (i.e., patching) shall be used instead of taking the mitigation path.

13.2.2 Summary of Considerations

Important considerations include:

1. Controlling the pathway to get the patch into the environment
2. System impacts, e.g., will a reboot be required.
3. System outage, i.e., reroute the traffic for the duration of the update
4. Notification of all parties, e.g., vendor, NG9-1-1 Entity, Service Provider
5. Sequential patch implementation process.

13.3 Appendix 3: NG9-1-1 “Entity” Architecture, Design, Engineering Change Control and Documentation

13.3.1 NG9-1-1 “Entity” Architecture, Design, Engineering Change Control and Documentation

Within an NG9-1-1 “Entity”, its internal network and associated security framework constitutes the core NG9-1-1 network architecture. Such intranet design may be further extended to other realms “NG9-1-1 network interconnection with other Network Domains diagram. NG9-1-1 “entities” may have multiple business relationships with other (mostly untrusted) Administrative Domain/Network Domains using IP wide-area network (WAN). The combined functions jointly performed by multiple domains form the architecture framework for E911 service.

13.3.1.1 Architecture Related to Inter-organizational Trust Relationship

Any trust, e.g., personnel, overall security posture, integrity of the networking, cannot be extended outside the local NG9-1-1 Entity organization or its “trust domain” without proper controls. Under careful review, there may be a subset of trust (e.g., allowing inter-NG9-1-1 Entity application-to-application data exchange after proper authentication, authorization, and accounting/auditing) can be established.

A classic case of extending the trust is the linking of Windows Networked Environment to another environment outside the local NG9-1-1 Entity.

Note that Windows Networking is a group of application-layer service based on ease-of-use and simplicity principle. A simple mouse “click” may have a potential extending the trust without this administrative user’s full acknowledgement of the new risks just being committed. Thus by default such environment shall not be extended outside NG9-1-1 Entity boundary without addressing the security architecture and implementation sufficiently.

The standard security best practices are:

1. Use Application Firewall controlling Windows services riding on top of NetBIOS over TCP/IP (NBT)
2. Do not extend any Trust Relationship beyond local NG9-1-1 Entity’s Windows Domain structure, i.e., broadening the security realm
3. Do not extend the Authentication, Authorization, and Accounting/Auditing (AAA) activity beyond the local NG9-1-1 Entity, nor shall accept others AAA result
4. Be careful on Active Directory structure and do restrict on information disclosure or unauthorized modification
5. Do not allow other Windows facilities (e.g., RRAS, Data Replication) outside the local NG9-1-1 Entity

13.3.1.2 Central-Server Based Communication

There are times certain communication methods will always go through servers hosted at Application Service Providers (ASPs) which serves as a switch board or relay host and information need to be passed through two end-points will go through the central server.

Some of the implementations are near real-time, while others are using a store-and-forward paradigm. In a mature service, such central servers perform tasks to ensure that service's production continuity, abuse avoidance, security enforcement, and cross-domain contamination suppression are all in place. One example is a sanctioned email service bureau, which will relay emails only after anti-spam filter, virus-scrubbing, and email content sanitization is applied.

For individual NG9-1-1 Entities, there may be resource constraints to deploy such a well-rounded central server to perform these complicated add-on functions. It certainly makes sense to use a sanctioned, security-approved service bureau as a service provider while individual NG9-1-1 Entities are simply subscribers of such service.

For new forms of communication, e.g., SMS, MMS messaging, pager, Blackberry, a gateway function shall be there to establish the linkage in between these messaging domains and the traditional IP-enabled service domain. Such gateway may be the most appropriate location to perform the necessary filtering and policy enforcement functions. The above example is used to illustrate how to include a new communication method into an acceptable NG9-1-1 Entity information feed.

As another example, Instant Messaging (IM) is a form of communication methods. Most of the IM services do go through a central server. A mature service provider does have some of the security enforcement features as described in secured email gateway above. Some of the service features (e.g., allowing transferring a file or installing a software) can be selectively turned-off. They are all driven by the central server configuration and policy applied. The common approach is to take the "Enterprise IM" solution where the policy is enforceable, the design is sanctioned, the user-community is controlled, and the peering user community (if it is allowed) is on the white-list.

13.3.1.3 Information Delivery Characteristics

One class of the communication methods is the store-and-forward delivery method⁶ commonly known as "messaging". In this class, information (e.g., request for emergency assistance) may be relayed from one or more "relay hosts" with various delivery priorities before reaching the NG9-1-1 Entity domain. The end-to-end propagation delay may spread in between near-real-time to a lengthy (e.g., more than 12 hours) delay and there is no positive "Acknowledgment"

⁶ Usually there is just one queue for processing/delivery. I.e., there is no priority treatment nor enforcement on prioritization

feedback⁷ from the final intended recipient⁸. Actually, such message may even be scrubbed by a spam filter or anti-virus filter⁹ anywhere en-route by a relay host. Bear in mind the end-user has to be trained to read¹⁰ the message (e.g., email) within a short period acceptable by the E9-1-1 service.

Another communication method is near real-time, two-way interactive system. This can be a POTS call, VoIP call, online-chat (generic term: instant messaging), or TDD call¹¹. The characteristic is there will always be a positive feedback by a 9-1-1 call-taker.

⁷ Receiving an indication of “Message Sent” from an intermediate relay host does not mean the end point actually has received or the recipient seen the message

⁸ Even if the final email server has received the message does not mean the actual person will (1) retrieve such message and (2) open-and-read such message

⁹ A message might be deleted or placed in a quarantine folder, if it is been allegedly detected as carrying a virus.

¹⁰ Message reader client software usually does not have an automatic priority screening function such that an emergency message embedded in the stream of messages can be moved ahead and read by the NG9-1-1 Entity call takers.

¹¹ This does not include call forwarded to an answering recorder system or an offline forwarder system, since these systems de-rate the response time equivalent to a store-and-forward system.

13.4 Appendix 4: Risk Acceptance & Approval Form

<i>13.4.1.1.1.1 Request and Requestor Information</i>			
Name			
Title			
Company			
Address			
Contact Number			
Email Address			
Date Requested			
Urgency	High	Medium	Low
Date Needed			
Duration of Risk	30 Days	60 Days	90 Days

Risk Justification:

Make a business case justifying the risk.

Risk Identification:

Description of the risk

--

Vulnerability Assessment:

Vulnerability	Type of Access (User ID) Required	Vulnerability Assessment
Unauthorized access or improperly controlled access through a filtering device.	None General Administrative	High Medium Low
Unauthorized access or improperly controlled access to an Administrative User ID.	None General Administrative	High Medium Low
Unauthorized access or improperly controlled access to a General User ID.	None General Administrative	High Medium Low
Unauthorized access or improperly controlled access to sensitive (Internal Use Only) Information	None General Administrative	High Medium Low
Unauthorized access or improperly controlled access to sensitive (Restricted) Information	None General Administrative	High Medium Low
Unauthorized access or improperly controlled access to sensitive (Most Sensitive Information)	None General Administrative	High Medium Low
Denial of service attack affecting systems, users, or services that are not local to the device under attack.	None General Administrative	High Medium Low

Denial of service attack affecting only systems, users, or services that are local to the device under attack.	None	High
	General	Medium
	Administrative	Low

Definitions for the above table:

- Filtering devices include: Routers, firewalls, other network components and operating systems capable of restricting access through that device by means of filters, access control lists, etc. For example: Cisco router ACL, Checkpoint Firewall-1 rule set.
- Administrative User ID: Any User ID having either system administrative, or security administrative authority. For example: UNIX root, Windows Administrator.
- General User ID: Any User ID not falling into the "Administrative User ID" category.

Impact Assessment:

Determine the inventory of assets that could be affected.

High Medium Low

Reasoning behind how the rating was obtained:

Threat Assessment:

Determine the likelihood of the vulnerability under consideration being exploited.

High Medium Low

Reasoning behind how the rating was obtained:

Overall Risk Assessment:

Determine the overall level of risk based on the combined ratings of Vulnerability, Impact, and Threat Assessments.

High

Medium

Low

Risk Analysis:

Document the comparison between the costs of eliminating the risk with the potential losses posed by the threats.

Risk Mitigation:

Document what strategy will be used, how, why, and when is it expected to last until. The exact approach (e.g., elimination, reduction, transference, or acceptance) shall be clearly specified in this section.

Review Period:

Based on the Overall Risk Assessment (High, Medium, Low), a re-review period of 3, 6, or 12 months will be assigned. Document the exact expiration date (from the date of the first signature on this form). **Make sure all parties involved are aware the re-approval period. All parties shall adhere to the same procedural formality as initial exception approval and risk acceptance. Failure to review leads to a state of non-compliance.**

Signatures:

Sign to certify that this is an accurate assessment of the identified risk

<i>13.4.1.1.1.2 NG9-1-1 Security Risk Manager</i>	
Name	
Title	
Organization	
Date	
Signature	

Sign to certify concurrence that this is believed to be an accurate assessment of the identified risk only after the Security Risk Manager has signed.

<i>13.4.1.1.1.3 Subject Matter Expert</i>	
Name	
Title	
Organization	
Date	
Signature	

Sign to acknowledge approval of the identified risk only after the Security Risk Manager and the Subject Matter Expert have signed. By signing this form, this approver is accepting complete accountability for the identified risk and commitment to the plan as defined in the Risk Mitigation section.

<i>13.4.1.1.1.4 NG9-1-1 Risk Acceptance Approver (Executive or Senior Manager)</i>	
Name	
Title	
Organization	
Date	
Signature	

14 Previous Acknowledgments

NA, this is Version 1.

SIP-PBX / Service Provider Interoperability

"SIPconnect 1.1 Technical Recommendation"

SIP Forum Document Number: TWG-2

Abstract

The SIPconnect 1.1 Technical Recommendation is a profile of the Session Initiation Protocol (SIP) and related media aspects that enables direct connectivity between a SIP-enabled Service Provider Network and a SIP-enabled Enterprise Network. It specifies the minimal set of IETF and ITU-T standards that must be supported, provides precise guidance in the areas where the standards leave multiple implementation options, and specifies a minimal set of capabilities that should be supported by the Service Provider and Enterprise Networks.

SIPconnect 1.1 effectively obsoletes SIPconnect 1.0. Where SIPconnect 1.0 focused primarily on basic network registration, identity/privacy management, call originations and call terminations, this version provides additional guidance on advanced service inter-working – including, but not limited to, call forwarding, call transfer, caller id, etc.

Where appropriate, recommendations from SIPconnect 1.0 have been left unchanged, although some modifications to prior recommendations have been made based on experience and feedback gathered through adoption of SIPconnect 1.0 in the industry.

Status of this Memo

SIPconnect 1.1 FINAL (v27).

Disclaimer

The SIP Forum takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the SIP Forum's procedures with respect to rights in SIP Forum Technical Recommendations, both drafts and final versions, or other similar documentation can be found in the SIP Forum's current adopted intellectual property right Recommendation. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this Technical Recommendation can be obtained from the SIP Forum.



S. Dawkins (Editor)
Huawei (USA)



SIPconnect and SIPconnect Compliant are certification marks of the SIP Forum. Implementers who wish to certify their products and services as SIPconnect Compliant may do so under the SIPconnect Compliant program of the SIP Forum. To learn more about this opportunity and obtain other useful information about SIPconnect, please visit www.sipforum.org/SIPconnect.

Table of Contents

Abstract	1
Status of this Memo	1
Disclaimer	1
Table of Contents	3
List of Figures	5
1 Introduction.....	6
2 Conventions and Terminology	7
3 Reference Architecture	7
4 Definitions	9
5 Key Assumptions and Limitations of Scope.....	9
6 Basic SIP Support.....	11
7 Modes of Operation	11
8 Supported Signaling Transport Protocols	13
8.1 TLS	13
9 Enterprise Public Identities.....	14
9.1 Routing SIP Requests to Enterprise Public Identities.....	14
10 Establishing Basic 2-Way Calls.....	14
10.1 Incoming Calls from the Service Provider to the Enterprise	15
10.1.1 Request-URI.....	15
10.1.2 "To" header field	15
10.1.3 "From" header field	15
10.1.4 "P-Asserted-Identity" and "Privacy" header fields.....	16
10.2 Outgoing Calls from the Enterprise to the Service Provider.....	17
10.2.1 Request-URI.....	17
10.2.2 "To" header field	18
10.2.3 "P-Asserted-Identity" header field	18
10.2.4 "From" header field	18
10.2.5 "Privacy" header field	18
11 Call Forwarding	19
12 Call Transfer	20
12.1 Overview.....	20
12.1.1 Blind transfer.....	20
12.1.2 Attended transfer	21
12.2 Requirements for use of the re-INVITE method in the context of call transfer.....	22
13 Emergency Services.....	22
14 Media and Session Interactions	23
14.1 SDP Offer/Answer	23
14.2 Codec Support and Media Transport	24
14.3 Transport of DTMF Tones.....	25
14.4 Echo Cancellation	25

14.5	FAX Calls	25
14.6	Call Progress Tones	25
14.7	Ringback Tone and Early Media.....	26
14.8	Putting a Session on Hold	26
15	Annex A: Registration Mode.....	27
15.1	Locating SIP Servers.....	27
15.1.1	Enterprise Requirements	27
15.1.2	Service Provider Network Requirements	27
15.2	Signaling Security	28
15.2.1	The use of transport=tls parameter.....	29
15.3	Firewall and NAT Traversal	29
15.4	Registration.....	29
15.4.1	Registration Failures	30
15.4.2	Registration-related failures for other requests	32
15.5	Maintaining Registration.....	32
15.6	Authentication.....	32
15.6.1	Authentication of the Enterprise by the Service Provider	32
15.6.2	Authentication of the Service Provider by the Enterprise	33
15.6.3	Accounting	33
15.7	Routing Inbound Requests to the SIP-PBX	33
16	Annex B: Static Mode	34
16.1	Locating SIP Servers.....	34
16.1.1	Enterprise Requirements	34
16.1.2	Service Provider Network Requirements	35
16.2	Signaling Security	35
16.3	Firewall and NAT Traversal	36
16.4	Failover and Recovery	37
16.5	Authentication.....	37
16.6	Routing Inbound Requests to the SIP-PBX	37
17	Appendix: Topics Not Addressed in SIPconnect 1.1.....	37
17.1	IPv6.....	37
17.2	UDP.....	38
17.3	Emergency Services.....	39
17.4	FAX Over IP	39
17.5	Service Provider-hosted Voice Mail	39
	References	40
18	Acknowledgements for SIPconnect 1.1 Initial Contributions	43
19	Contributors to SIPconnect 1.1 and Contact Information.....	43
20	Acknowledgements to Contributors to SIPconnect 1.0	44
21	Full Copyright Statement.....	44

List of Figures

1. Figure 1: Reference Architecture	7
2. Figure 2: Call Forward	19
3. Figure 3: Blind Transfer	21
4. Figure 4: Attended Transfer	22

1 Introduction

The Session Initiation Protocol (SIP) is fast becoming the dominant industry standard for signaling in support of VoIP and other services. The deployment of Session Initiation Protocol (SIP)-enabled PBXs (SIP-PBXs) among Enterprises of all sizes is increasing rapidly. Deployment of SIP infrastructure by Service Providers is also increasing, driven by the demand for commercial VoIP offerings. Many new SIP-PBXs support SIP phones and SIP-based communication with other SIP-PBXs. The result of these parallel deployments is a present need for direct IP peering between SIP-enabled SIP-PBXs and Service Providers.

Currently published ITU-T Recommendations and IETF RFCs offer a comprehensive set of building blocks that can be used to achieve direct IP peering between SIP-enabled SIP-PBX systems and a Service Provider's SIP-enabled network. However, due to the sheer number of these standards documents, Service Providers and equipment manufacturers have no clear "master reference" that outlines which standards they must specifically support in order to ensure success. This has led to a number of interoperability problems and has unnecessarily slowed the migration to SIP as replacement for traditional TDM (Time Division Multiplexed) connections.

This SIP Forum document aims to address this issue. In short, this document defines the protocol support, implementation rules, and features required for predictable interoperability between SIP-enabled Enterprise Networks and SIP-enabled Service Providers. Note that this document does not preclude or discourage the negotiation of additional functionality.

SIPconnect 1.1 restates, updates, and extends the areas of implementation guidance found in SIPconnect 1.0, including:

- Specification of a reference architecture that describes the common network elements necessary for Service Provider-to-SIP-PBX peering for the primary purpose of call origination and termination.
- Specification of the basic protocols (and protocol extensions) that must be supported by each element of the reference architecture.
- Specification of the exact standards associated with these protocols that must or should be supported by each element of the reference architecture.
- Specification of two modes of operation – Registration mode and Static mode - whereby a Service Provider can locate a SIP-PBX.
- Specification of standard forms of Enterprise Public Identities.
- Specification of signaling messages for Basic 2-Way Calls, Call Forwarding, and Call Transfer.
- Specification of minimum requirements for codec support, packetization intervals, and capability negotiation.
- Specification of minimum requirements for handling fax and modem transmissions.
- Specification of minimum requirements for handling echo cancellation.
- Specification of minimum requirements for transporting DTMF tones.
- Specification of basic security mechanisms.

2 Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC 2119\]](#)

3 Reference Architecture

The reference architecture diagram in Figure 1 shows the functional elements required to support the interface described in this Technical Recommendation. The diagram shows two reference points between the Enterprise Network and the Service Provider Network; reference point (1) and reference point (2).

Reference point (1) carries SIP signaling messages to support voice services between the Enterprise Network SIP-PBX and the Service Provider network SIP Signaling Entity (SP-SSE).

Reference point (2) carries the RTP and RTCP packets between the Service Provider and Enterprise Media Endpoints. An Enterprise Media Endpoint could be contained within a physical SIP-PBX, an IP-based user device (e.g., SIP phone) in the Enterprise, or a media-relay device in the Enterprise Network. The Service Provider Media Endpoint could be a PSTN Gateway, an IP-based user endpoint device, a media server, or any other IP-based media-capable entity.

Reference points (1) and (2) together comprise the SIPconnect 1.1 interface.

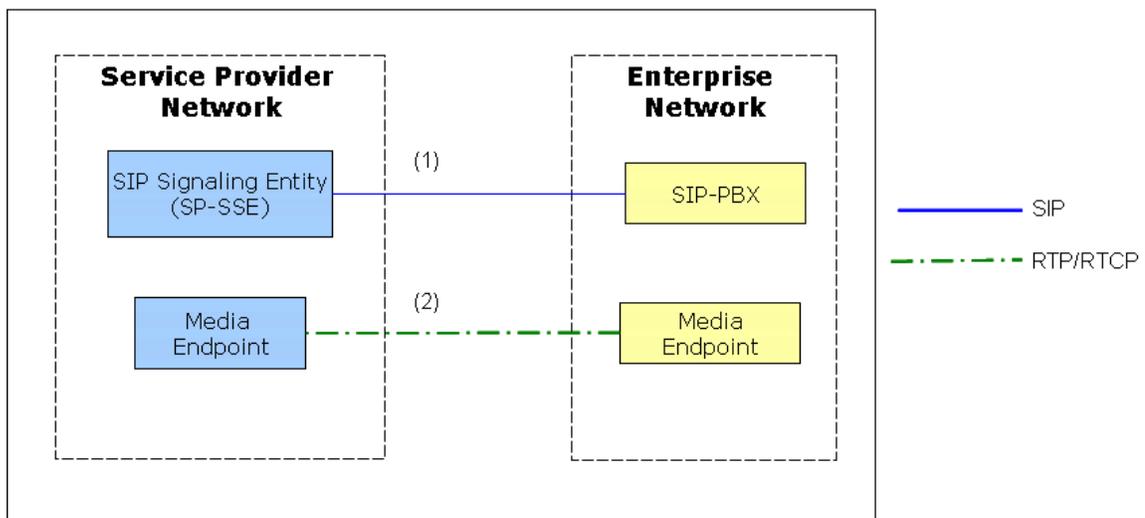


Figure 1: Reference Architecture

It is important to note that this Technical Recommendation treats these elements as separate physical components for the purposes of illustration only. It is perfectly acceptable for an equipment manufacturer

to combine a Media Endpoint with the corresponding signaling entity. For example, a manufacturer may choose to integrate the SIP-PBX and Media Endpoint functions. Both integrated and non-integrated implementations are equally conformant as long as they fully adhere to the individual rules governing each of the defined functions.

Additionally, just as multiple logical functions can be collapsed into one physical entity, a single logical function in this Technical Recommendation can be decomposed into multiple physical entities. For example, the SP-SSE can be decomposed into a SIP registrar and a Session Border Controller (SBC). In this situation, however, the interface between the registrar and the SBC is internal to SP-SSE logical entity and is not covered by this Technical Recommendation.

Note that many deployments will include a Network Address Translator (NAT) between the Service Provider Network and the Enterprise Network. This document does not describe NATs as part of the SIPconnect 1.1 interface.

Note that a single SIP-PBX may serve Media Endpoints in a number of geographically-distributed locations.

4 Definitions

Service Provider SIP-Signaling Entity (SP-SSE) – the Service Provider’s point of SIP signaling interconnection with the Enterprise.

SIP-PBX – the Enterprise’s point of SIP signaling interconnection with the Service Provider.

SIP Endpoint – a term used in this specification to refer to both SP-SSEs and SIP-PBXes.

Enterprise Public Identity - an Address of Record (AOR) represented as a SIP URI, used to identify a user or group of users served by the SIP-PBX. Enterprise Public Identities are used in conjunction with delivering incoming and outgoing calls.

Registration AOR – An AOR represented as a SIP URI, used solely to identify the SIP-PBX during registration.

Media Endpoint – Any entity that terminates an RTP/RTCP stream.

Back-to-Back User Agent (B2BUA) –a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates a request to another SIP user agent server (UAS).

5 Key Assumptions and Limitations of Scope

This Technical Recommendation lists a number of IETF and ITU-T specifications needed to meet the requirements for interconnection between a Service Provider and an Enterprise Network.

The following key assumptions have been made:

- The primary service to be delivered over this interface is audio-based call origination and/or termination between the Enterprise and Service Provider Networks, including emergency services. The delivery of any other service (e.g. video-based services, instant messaging, etc.) is out of scope.
- All reference architecture elements specified for the Service Provider and Enterprise Networks are in place and operational.
- Signaling considerations between the SP-SSE and other Service Provider devices (e.g. Trunking Gateway) are outside the scope of this document.
- Signaling considerations between the SIP-PBX and other Enterprise devices (e.g. IP phones) are outside the scope of this document.

- Layer 3 network design and QoS considerations are outside of the scope of this document
- Element management, network management, network security, and other operational considerations are outside the scope of this document.

SIPconnect 1.1 is intended to support a SIP peering/trunking model, in which the Service Provider Network provides a SIP peering/trunking capability to a SIP PBX in an Enterprise Network, to enable communications between the Enterprise users served by the SIP PBX and users outside of the Enterprise Network. In the peering/trunking model, the Service Provider network may have knowledge of the set of Enterprise Public Identities associated with the SIP PBX as a whole and the SP-SSE has responsibility for the Registration AOR (if applicable), but the SIP PBX has responsibility for the Enterprise Public Identities and provides services to the individual Enterprise users.

A Hosted Services model (also called Centrex), in which the Service Provider has responsibility for the AORs associated with Enterprise Public Identities, and provides hosted services to individual enterprise users, is out of scope for SIPconnect 1.1.

6 Basic SIP Support

SIP-PBXs and SP-SSEs **MUST** support SIP in accordance with [\[RFC 3261\]](#) and offer-answer in accordance with [\[RFC 3264\]](#), as qualified by statements in later sections of this document. Requirements for support of other IETF RFCs and other standards are as stated in later sections of this document.

This document specifies a profile of SIP, as well as specifying some media aspects. Implementations of this Technical Recommendation **MUST NOT** simply assume that a particular feature or option listed as mandatory in this document is supported by a peer SIP-PBX or SP-SSE. Instead, a SIP-PBX or SP-SSE **MUST** use mechanisms specified for SIP (e.g., Supported, Require and Allow header fields) and SDP (e.g., attributes, payload formats) for ascertaining support of a given SIP or SDP extension at a peer SP-SSE or SIP-PBX. Failure to do this can lead to interoperability problems.

7 Modes of Operation

This document describes two modes of operation for SIPconnect 1.1; the Registration mode (specified in "Annex A", Section 15) and the Static mode (specified in "Annex B", Section 16). These modes differ primarily in the way the Service Provider Network discovers the SIP signaling address of the SIP-PBX.

In the Registration mode, the SIP-PBX conveys its SIP signaling address to the Service Provider Network using the SIP registration procedure defined in [\[RFC 6140\]](#). In effect, the SIP-PBX registers with the Service Provider Network, using a REGISTER request with a specially-formatted Contact URI. After the SIP-PBX is authenticated, the registrar updates its location service with a unique AOR-to-Contact mapping for each of the AORs associated with the SIP-PBX. The primary advantage of the Registration mode is that it enables the SIP-PBX to be easily deployed in a "plug-and-play" fashion; i.e., with only a minimum of configuration data the SIP-PBX can initiate the registration procedure to automatically establish connectivity with the Service Provider Network.

In Registration mode:

- The SIP-PBX uses SIP registration procedures to advertise the SIP-PBX's SIP signaling address to the SP-SSE, and
- The SP-SSE authenticates the SIP-PBX using SIP Digest.

In the Static mode, the Service Provider Network views the SIP-PBX as a peer SIP-based network that is responsible for the Enterprise Public Identities that it serves. In this mode the Service Provider Network is either configured with the SIP-PBX signaling address, or it discovers the address using the Domain Name Service (DNS). The Service Provider Network procedures for routing out-of-dialog requests to the SIP-PBX align closely with the SIP routing procedures defined in [\[RFC 3261\]](#) (and [\[RFC 3263\]](#) if DNS is used).

In Static mode:

- The Enterprise Network can use DNS to advertize its publicly-reachable SIP-PBX SIP signaling address to the SP-SSE.

Advantages of Registration mode over Static mode include:

- It enables the Service Provider Network to discover the signaling address of the SIP-PBX that is assigned a dynamic IP address (so that the SIP-PBX is not required to have a static signaling address publicly viewable in DNS),
- It provides a mechanism for a SIP-PBX located behind a NAT to automatically establish connectivity with the Service Provider Network,
- It provides a mechanism for a failed SIP-PBX to automatically inform the network when it is back online, and
- It enables the Service Provider to tap into streamlined and scalable subscriber provisioning and management processes (e.g., a Service Provider Network that is designed to support the heavy registration traffic generated by millions of users is well suited to support registration traffic generated by large numbers of SIP-PBXs operating in the Registration mode).

Advantages of Static mode over Registration mode include:

- Since Static-mode SIP-PBXes do not send REGISTER requests when they initialize, Static mode operation is less susceptible to "avalanche restart" issues, when a large geographic area restores power, and
- The SP-SSE is not dependent on the SIP-PBX to re-establish any broken registration before the SP-SSE can deliver inbound requests to the SIP-PBX.

The Static mode is often used for larger Enterprises, where the size of the Enterprise warrants more explicit provisioning of connection and service information by the Service Provider. For example, large Enterprise trunks often have unique requirements for SLAs (Service Level Agreements), call routing, load balancing, codec support, etc., which make explicit provisioning necessary.

SIP-PBXs **MUST** support either Registration mode, as specified in Annex A, or Static mode, as described in Annex B. SIP-PBXs **MAY** support both modes,

SP-SSEs **MUST** support either Registration mode, as specified in Annex A, or Static mode, as described in Annex B. SP-SSEs **MAY** support both modes.

Note that an SP-SSE supporting only Annex A and a SIP-PBX supporting only Annex B, or vice versa, will not interoperate. Both sides must support the same Annex in order to communicate.

8 Supported Signaling Transport Protocols

SIP-PBXs and SP-SSEs **MUST** implement TCP. TCP does not have to be **used** for a SIPconnect 1.1 signaling connection, if both sides agree not to, but it must be available in order to comply with this Technical Recommendation.

UDP support is allowed in order to accommodate legacy devices. TCP support is mandated in order to accommodate large and growing SIP requests and responses (see Section 17.2 for more background), and for use with TLS.

8.1 TLS

The SIP-PBX and SP-SSE **MUST** support Transport Layer Security (TLS) v1.0 as described in [\[RFC 2246\]](#) and [\[RFC 3261\]](#). While SIPconnect 1.1 continues to require TLS support at **MUST** strength, we should note that using TLS for signaling as described in Sections 15.2 and 16.2 does not require the use of the SIPS URI scheme.

[\[RFC 3261\]](#) Section 26.2.2 deprecates the "transport=TLS" URI parameter. SIP-PBXes and SP-SSEs **MUST** ignore this parameter.

When presenting a certificate, a SIP-PBX or SP-SSE **SHOULD** identify itself by means of a SIP URI using type uniformResourceIdentifier in the subjectAltName field, in accordance with [\[RFC 5280\]](#).

[\[RFC 3261\]](#) Section 26.3.1 states:

Proxy servers, redirect servers, and registrars **SHOULD** possess a site certificate whose subject corresponds to their canonical hostname.

When receiving a certificate, SIP-PBX or SP-SSE implementations **MUST** support extraction of the canonical hostname from the subjectCommonName (CN) if (and only if) it is not present in the subjectAltName. SIP-PBX and SP-SSE implementations **MUST** comply with guidelines relating to usage of the Subject field, specified in RFC 5280 Section 4.1.2.6, and the SubjectAltName field as specified in [\[RFC 5280\]](#) Section 4.2.1.6. Compliance with [\[RFC 5280\]](#) Section 4.1.2.6 is necessary to support existing certificate signer implementations that use the CN field instead of the subjectAltName field.

Furthermore, SIP-PBX and SP-SSE implementations **MUST** be able to accept a DNS name as an identity (e.g. proxy1.example.com), instead of a SIP URI as defined in [\[RFC 3261\]](#) (e.g., sip:proxy.example.com). This is to allow for supporting SP-SSE or SIP-PBX implementations that commonly use certificates that were created for HTTP instead of for SIP. It is also **RECOMMENDED** that SIP-PBX and SP-SSE implementations be able to provide a certificate with either a URI or DNS name for backward compatibility.

9 Enterprise Public Identities

SIP-PBXs and SP-SSEs **MUST** be able to support Enterprise Public Identities in the form of a SIP URI containing a global E.164 [\[ITU-T E.164\]](#) number and the "user=phone" parameter.

For example:

sip:+16132581234@example.com;user=phone

The global E.164 number **MUST** begin with a leading "+", **MUST NOT** contain a phone-context parameter and **MUST NOT** include visual separators.

For a given SIPconnect 1.1 interface, the choice of value for the host part of Enterprise Public Identities is a contractual matter between the enterprise and the Service Provider. For Registration mode, the value of the host part of Enterprise Public Identities will be the domain name or sub-domain name of the Service Provider. For Static mode, the value of the host part of Enterprise Public Identities can be in the form of a sub-domain of the Service Provider domain assigned to the SIP-PBX (e.g. "pbx1.operator.net"), or the SIP-PBX IP address, or the domain of the Enterprise (e.g. "enterprise.com").

Support for other forms of Enterprise Public Identity (including identities based on telephone numbers that are not global E.164 numbers (e.g., sip:7042;phone-context=enterprise.com@example.com;user=phone) and identities not based on telephone numbers (e.g., sip:alice@example.com) is out of scope of this Technical Recommendation.

9.1 Routing SIP Requests to Enterprise Public Identities

The SP-SSE is responsible for routing SIP requests to the appropriate SIP-PBX; i.e. on receiving a SIP request addressed to an Enterprise Public Identity, the SP-SSE must use the received Enterprise Public Identity to discover the SIP signaling address of the SIP-PBX. The mechanism to perform this discovery depends on whether the SIP-PBX is deployed using Registration or Static mode:

- In Registration mode, the SP-SSE determines the SIP-PBX signaling address using the address binding that was established when the SIP-PBX registered, as described in Section 15.
- In Static mode the SP-SSE determines the SIP-PBX signaling address using either statically configured data or DNS, as described in Section 16.

10 Establishing Basic 2-Way Calls

This section describes the procedures for establishing basic 2-way calls between the Enterprise and the Service Provider Network.

10.1 Incoming Calls from the Service Provider to the Enterprise

Calls to Enterprise Public Identities are routed by the SP-SSE to the SIP-PBX and are usually routed by the SIP-PBX directly to a specific user station – bypassing the attendant or operator. This is commonly referred to as "Directed Inward Dial" (DID) service.

This section describes guidelines for populating the Request-URI, and the "P-Asserted-Identity" [[RFC 3325](#)] and [[RFC 5876](#)], "To" and "From" header fields for new-dialog INVITE requests sent from the SP-SSE to the SIP-PBX. The SP-SSE **MUST** ensure that all other header fields in the INVITE request comply with [[RFC 3261](#)].

10.1.1 Request-URI

The SP-SSE **MUST** populate the Request-URI of the INVITE request in accordance with Section 15.7 for Registration mode and in accordance with Section 16.6 for Static mode.

On receiving an INVITE request from the SP-SSE, the SIP-PBX **MUST** identify the called user based on the contents of the Request-URI.

10.1.2 "To" header field

The "To" header field URI of a SIP request generated by the SP-SSE is frequently populated with the Enterprise Public Identity to which the Request-URI relates. However, there may be cases, such as a prior redirection, where the "To" header field URI does not contain the desired destination. As such, the SIP-PBX **MUST NOT** rely on the contents of "To" header field for routing decisions, but **MUST** use the Request-URI instead.

10.1.3 "From" header field

For IP-based originations, there are no special restrictions on the contents of the "From" header field URI, beyond the requirements specified in [[RFC 3261](#)]. For example, the "From" header field URI could contain either a SIP or Tel URI. Typically the "From" header field URI is set by the originating UAC, and either carried transparently through to the terminating UAS, or modified en-route. For example, a network-based "anonymizing" service could update the "From" header field URI to obscure the identity of the caller and originating Service Provider. In cases where the SP-SSE needs to generate an anonymous URI (e.g., for a call incoming to the Service Provider Network from the PSTN for which calling number privacy is requested), the SP-SSE **MUST** send a URI as shown here.

sip:anonymous@anonymous.invalid

Note: Where a display-name is included, no semantic meaning should be attributed to the display name. This has resulted in reported interoperability problems, because the display name could be in any language.

If the originating SIP entity supplied an E.164 calling number, and the caller did not request calling number privacy, then the SP-SSE **MUST** populate the "From" header field with a SIP URI containing the E.164 calling number, the Service Provider domain name, and the "user=phone" parameter as shown below. If any display name information is available and has not been restricted for delivery, it **SHOULD** also be provided.

sip:+15616261234@example.com;user=phone

where "example.com" is the domain name of the Service Provider Network.

If no caller identity is available and privacy has not been requested, the SP-SSE **SHOULD** send a URI containing a host portion with a top level domain of ".invalid", as shown below.

unavailable@unknown.invalid

There are no special requirements placed on the SIP-PBX in processing the "From" header field, beyond the requirements specified in [\[RFC 3261\]](#).

10.1.4 "P-Asserted-Identity" and "Privacy" header fields

If the caller requested privacy, and the Service Provider Network does not trust the Enterprise Network, then the SP-SSE **MUST** remove all "P-Asserted-Identity" header fields in the INVITE request before sending the request to the SIP-PBX.

If the caller requested privacy, and the SP-SSE is able to assert an identity, and the Service Provider Network trusts the Enterprise Network, then the SP-SSE **MUST** include a "P-Asserted-Identity" header field and a "Privacy" header field with value 'id' in the INVITE request, in addition to providing an anonymous "From" header field URI as specified in Section 10.1.3, before sending the request to the SIP-PBX.

If the caller did not request privacy, and the SP-SSE is able to assert an identity, then the SP-SSE **MUST** include a "P-Asserted-Identity" header field containing a URI identifying the calling user in the INVITE request before sending the request to the SIP-PBX.

In general, there are no restrictions on the contents of the "P-Asserted-Identity" header field, beyond the requirements specified in [\[RFC 3325\]](#) and [\[RFC 5876\]](#). This is due to the fact that when the SP-SSE receives a "P-Asserted-Identity" header field from a trusted entity that conforms to [\[RFC 3325\]](#) and [\[RFC 5876\]](#), it transparently passes the header field to the SIP-PBX without modification. This means that the SIP-PBX **MUST** support receiving a "P-Asserted-Identity" header field containing any form of URI permissible according to [\[RFC 3325\]](#) and [\[RFC 5876\]](#).

The "domain-name" identifies the domain of the originating network; e.g. "domain-name" could be domain of the Service Provider Network, domain of a peer to the Service Provider Network, or domain of

another Enterprise Network. As described in [\[RFC 3325\]](#), the SIP-PBX **MUST** accept up to two "P-Asserted-Identity" header fields, one in the form of a Tel URI, and one in the form of a SIP URI, and **MUST** prefer the SIP URI when two are present.

If the "P-Asserted-Identity" header field is to be included, then the SP-SSE **SHOULD** also include display name information along with the SIP or Tel URI in the "P-Asserted-Identity" header field, if the display name is available and has not been restricted for delivery.

For example:

P-Asserted-Identity: "John Smith" <sip:+15616261234@example.com;user=phone>

The SIP-PBX **MUST** support receiving a "Privacy" header field from the SP-SSE that contains a priv-value of either 'id' or 'none', as per [\[RFC 3325\]](#), [\[RFC 5876\]](#) and [\[RFC 3323\]](#).

10.2 Outgoing Calls from the Enterprise to the Service Provider

This section describes SIP-PBX and SP-SSE requirements for populating and receiving the Request-URI and "To" and "From" header fields for new dialog INVITE requests sent from the SIP-PBX to the SP-SSE. It also specifies how the "P-Asserted-Identity" header field can be used by the Enterprise Network to assert the identity of the caller, and usage of the "Privacy" header field to suppress the delivery of caller identity, as described in [\[RFC 3325\]](#) and [\[RFC 5876\]](#). The SIP-PBX **MUST** ensure that all other header fields in the INVITE request comply with [\[RFC 3261\]](#).

This section covers the case where the call is initiated by an Enterprise user served by the SIP-PBX. The case where the SIP-PBX sends an INVITE request to the SP-SSE to establish the forward-to leg of a call forwarded by an Enterprise user is covered in Section 11.

10.2.1 Request-URI

If the SIP-PBX has an E.164 number identifying the called user (e.g., derived from a Tel URI or a dial string), the SIP-PBX **MUST** populate the Request-URI of the INVITE request with a SIP URI of the following form, using the domain name of the Service Provider in the host part:

sip:+12128901234@sp.example.com;user=phone

If the SIP-PBX has a dial string identifying the called user and is unable to convert it to a SIP URI of the "user=phone" form, the SIP-PBX **MUST** populate the Request-URI of the INVITE request with a SIP URI in the following form:

sip: 92125551212@sp.example.com

10.2.2 "To" header field

The "To" header field URI in a SIP request generated by the SIP-PBX is normally populated with the same URI as the Request-URI. However, there may be cases, such as a prior redirection, where the "To" header field URI does not contain the desired destination. As such, the SP-SSE **MUST NOT** rely on the "To" header field URI for routing decisions, but use the Request-URI instead.

10.2.3 "P-Asserted-Identity" header field

The SIP-PBX **MUST** include a "P-Asserted-Identity" header field in the INVITE request in accordance with the rules of [\[RFC 3325\]](#) and [\[RFC 5876\]](#) unless the SIP-PBX needs to withhold the identity for privacy reasons or the SIP-PBX is performing call forwarding and is unable to assert the identity of the original caller. The header field could contain an Enterprise Public Identity in accordance with Section 9 or, if received from another trusted node, could contain some other SIP or Tel URI.

10.2.4 "From" header field

The SIP-PBX **MUST** populate the "From" header field URI with a URI that the SIP PBX wishes to be used for caller identification. This may be an Enterprise Public Identity, an anonymous URI, or a SIP or Tel URI that the SIP-PBX has received from an entity behind the SIP-PBX.

If the "From" URI is not an Enterprise Public Identity, the Service Provider's ability to deliver this information as caller identification will depend on policy.

In cases where the Enterprise Network needs to generate an anonymous URI on behalf of a caller (as opposed to passing on a received anonymous URI), the SIP-PBX **MUST** send a URI of the form

sip:anonymous@anonymous.invalid

10.2.5 "Privacy" header field

If the SIP-PBX requires privacy for a call by suppressing delivery of caller identity to downstream entities, it **MUST** include a "Privacy" header field with value 'id' in the INVITE request, in addition to providing an anonymous "From" header field URI as specified in Section 10.2.4. If the SP-SSE provides privacy by default and the SIP-PBX requires privacy to be overridden for a call, the SIP-PBX **MUST** include a "Privacy" header field with value 'none' in the INVITE request.

The SP-SSE **MUST** support receiving a "Privacy" header, from the SIP-PBX that contains a priv-value of either 'id' or 'none', as per [\[RFC 3325\]](#), [\[RFC 5876\]](#) and [\[RFC 3323\]](#).

11 Call Forwarding

The ability for the Enterprise to forward calls through the SIPconnect interface is considered a basic requirement. In order to forward a call, the SIP-PBX **MUST** send an INVITE request to the SP-SSE, populated as specified in Section 10.2, with the Request-URI identifying the forwarded-to target destination.

A simplified example call flow for Call Forwarding is shown in Figure 2. Note that the initial call leg is on dialog [1] and the forwarded leg is on dialog [2].

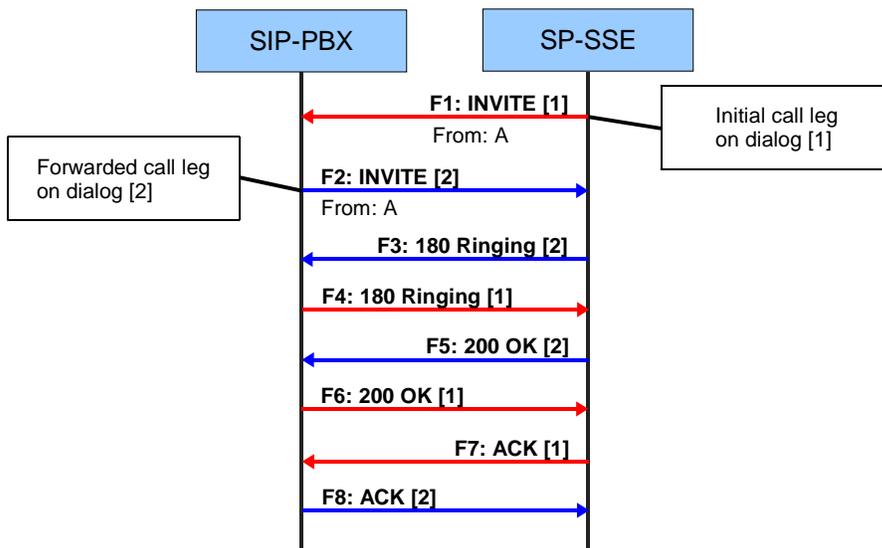


Figure 2: Call Forward

Note that the following provisions of Section 10.2 have particular relevance for forwarded calls:

- The "To" header field URI can identify the originally targeted destination, in which case it will not match the Request-URI;
- The "P-Asserted-Identity" header field can be absent or can assert an identity that is not an Enterprise Public Identity;
- The "From" header field URI can contain an identity that is not an Enterprise Public Identity.

An SP-SSE **MUST** be able to accept forwarded calls from a SIP-PBX. Note that an SP-SSE may enforce policies that include a variety of restrictions on calls forwarded from an untrusted SIP-PBX (e. g., mandating the inclusion of a "Diversion" header field [RFC 5806] with a "From" header field that does not correspond to an Enterprise Public Identity assigned to the SIP-PBX). These policies are outside the scope of the SIPconnect Technical Recommendation.

12 Call Transfer

The ability for the SIP-PBX or the SP-SSE to transfer calls that cross the SIPconnect 1.1 interface is considered a basic requirement in this Technical Recommendation. This section specifies a set of SIP primitives that can be used to support the transfer of calls that cross a SIPconnect 1.1 interface.

12.1 Overview

Call transfer can be accomplished by the use of REFER requests (a "proxy model") in accordance with [\[RFC 5589\]](#), or by the use of one or more INVITE/re-INVITE requests (a "third party call control model"). The SP-SSE and SIP-PBX **MUST** support the use of INVITE/re-INVITE for initiating and responding to call transfers.

Support for initiating and responding to call transfers using the REFER method is outside the scope of SIPconnect 1.1. SIPconnect 1.1 has selected the use of INVITE/re-INVITE for call transfer because that is what is commonly deployed at the time of writing and because of Enterprise or Service Provider policies that might require rejection of received REFER requests (e.g., because of charging considerations).

12.1.1 Blind transfer

Blind transfer, known as basic transfer in [\[RFC 5589\]](#), is where a new call is established from the transferee to the transfer target and the transferor drops out immediately, without waiting for the transfer target to answer.

A SIP-PBX acting as a B2BUA can accomplish blind transfer using INVITE/re-INVITE as follows. Assuming that the call with the transferee crosses the SIPconnect 1.1 interface and the transfer target is reachable across the SIPconnect 1.1 interface, the SIP-PBX sends a new dialog INVITE request to the SP-SSE targeted at the transfer target and sends a re-INVITE request to the SP-SSE on the existing dialog with the transferee, changing the SDP for this dialog, so media goes between the transferee and transfer target.

The SP-SSE can accomplish blind transfer in a similar manner using INVITE/re-INVITE. The INVITE and re-INVITE transactions are used to achieve an offer-answer exchange between the transferee and transfer target.

For example, the SIP-PBX can send an offerless INVITE request towards the transfer target. In response, the transfer target supplies an SDP offer, which the SIP-PBX includes in a re-INVITE request towards the transferee. The SIP-PBX then forwards the SDP answer from the transferee in an ACK request towards the transfer target. If the transferee is within the SIP-PBX, only the INVITE transaction towards the transfer target will cross the SIPconnect 1.1 interface. If the transfer target is within the SIP-PBX, only the re-INVITE request towards the transferee will cross the SIPconnect 1.1 interface.

A simplified example call flow for Blind Transfer is shown in Figure 3. Note that the initial call leg is on dialog [1] and the transferred leg is on dialog [2]. It should be noted that this call flow is illustrative only, and does not mandate a specific implementation. More complex call flows may be required to support feature interactions encountered in real-world deployments; for example when the transfer target has a terminating feature that sends early media toward the transferee.

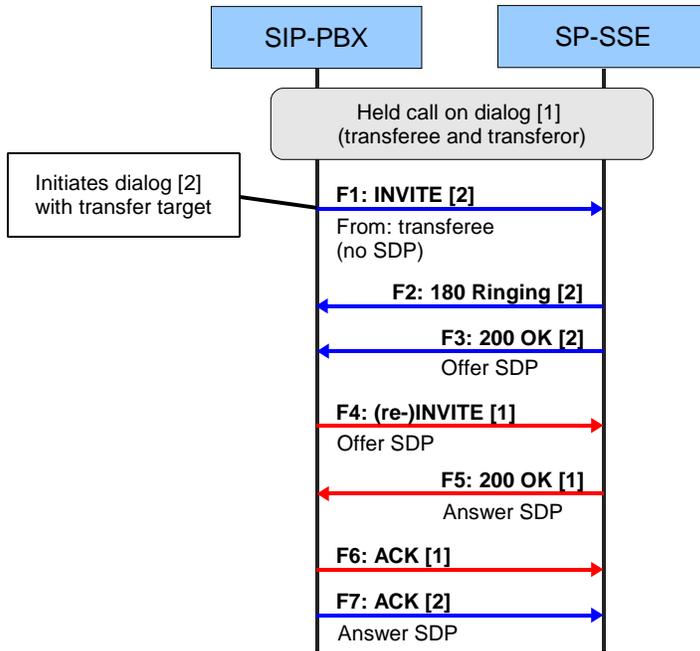


Figure 3: Blind Transfer

Requirements for the support of re-INVITE are given in Section 12.2.

12.1.2 Attended transfer

Attended transfer is where the transferor has already established a new call to the transfer target and the transfer target has answered. Transfer then involves replacing the two existing calls (with the transferee and with the transfer target) by a single call.

The SIP-PBX can accomplish attended transfer using re-INVITE as follows. Assuming that each call crosses the SIPconnect 1.1 interface, the SIP-PBX sends a re-INVITE request to the SP-SSE on each of the existing dialogs. The two re-INVITE transactions are used to achieve an offer-answer exchange between the transferee and transfer target.

For example, the SIP-PBX can send an offerless re-INVITE request towards the transfer target. In response, the transfer target supplies an SDP offer, which the SIP-PBX includes in a re-INVITE request towards the transferee. The SIP-PBX then forwards the SDP answer from the transferee in an ACK

request towards the transfer target. If the transferee is within the SIP-PBX, only the re-INVITE transaction towards the transfer target will cross the SIPconnect 1.1 interface. If the transfer target is within the SIP-PBX, only the re-INVITE transaction towards the transferee will cross the SIPconnect 1.1 interface. A simplified example call flow for Attended Transfer is shown in Figure 4. Note that the initial call leg is on dialog [1] and the transferred leg is on dialog [2].

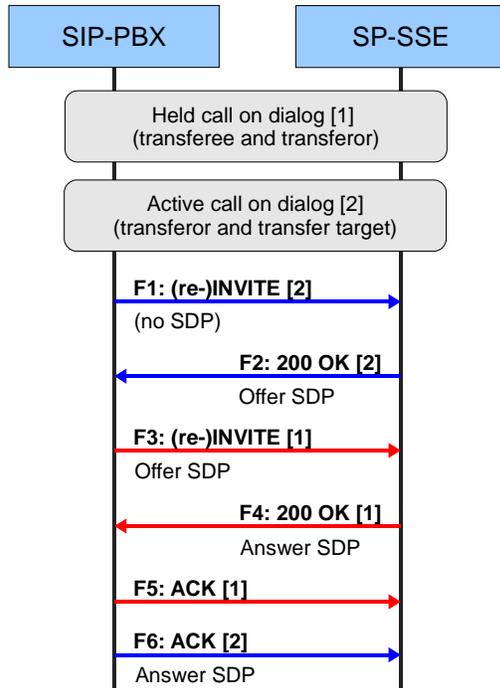


Figure 4: Attended Transfer

The SP-SSE can accomplish attended transfer in a similar manner using re-INVITE.

Requirements for the support of re-INVITE are given in Section 12.2.

12.2 Requirements for use of the re-INVITE method in the context of call transfer

The SIP-PBX and the SP-SSE **MUST** support both sending and receiving a re-INVITE request with an SDP offer, and sending and receiving a re-INVITE request without an SDP offer.

13 Emergency Services

The SIP-PBX **MUST** have a dial plan that recognizes emergency calls.

When a SIP-PBX routes a call recognized as an emergency call to the SP-SSE, it **MUST** populate the Request-URI using a dial string URI, as specified in Section 10.2.1, that contains the national emergency services number.

The SIP PBX **MUST** include the identity of the caller in the "P-Asserted-Identity" header field, as described in Section 10.2.3, and in the "From" header field, as described in Section 10.2.4, except in territories where the SIP-PBX is required to include other information (such as a Location Identification Number) in one of these header fields. The SIP PBX **MUST NOT** withhold the "P-Asserted-Identity" header field for privacy reasons and **MUST NOT** anonymize the "From" header field.

The SP-SSE **MUST** be able to recognize emergency calls based on the presence of the agreed emergency services number in the Request-URI.

If an originating session is an emergency session, then SIP session limits do not apply. The SP-SSE **MUST NOT** apply SIP session limits to emergency calls originated by the SIP-PBX. Note that this does not preclude the SP-SSE rejecting the emergency call for other reasons including local congestion or exceeding limits explicitly applicable for emergency calls.

14 Media and Session Interactions

14.1 SDP Offer/Answer

A SP-SSE/SIP-PBX acting on behalf of a Media Endpoint that originates and/or terminates RTP traffic **MUST** utilize the Session Description Protocol (SDP) as described in [\[RFC 4566\]](#) in conjunction with the offer/answer model described in [\[RFC 3264\]](#) to exchange media capabilities (IP address, port number, media type, send/receive mode, codec, DTMF mode, etc).

SIP-PBXs and SP-SSEs **MUST** be capable of receiving INVITE requests without an SDP offer and supplying an SDP offer in an appropriate response, in accordance with [\[RFC 3261\]](#).

During a call, media capability negotiation may be initiated by either end, for the purpose of verifying dialog state or for other reasons, and experience has shown that some SIP implementations don't handle offers with unchanged SDP correctly.

A SP-SSE/SIP-PBX that participates in SDP offer/answer negotiation **MUST** be prepared to accept additional offers containing SDP with a version that has not changed, and **MUST** generate a valid answer (which could be the same SDP sent previously, or could be different).

A SP-SSE/SIP-PBX that sends additional SDP offers with the same version **MUST** be prepared to accept answers with SDP which may be the same as the previously received SDP, or may be different.

A SP-SSE/SIP-PBX that sends SDP with a change compared to the previously sent SDP **MUST** increase the version number in the o-line, in accordance with [\[RFC 4566\]](#).

SIP-PBX and SP-SSE implementations sending changes to negotiated media capabilities via SIP reINVITE **MUST** support [\[RFC 3261\]](#), Section 14 "Modifying an Existing Session". SIP UPDATE **MAY** be used for this purpose when both endpoints advertise support for [\[RFC 3311\]](#).

14.2 Codec Support and Media Transport

A Media Endpoint **MUST** transport and receive voice samples using the real-time transport protocol (RTP) as described in [\[RFC 3550\]](#).

Any Media Endpoint that originates and/or terminates RTP traffic over UDP **MUST** use the same UDP port for sending and receiving session media (i.e. symmetric RTP).

Any Media Endpoint that originates and/or terminates RTP traffic **MUST** be capable of processing RTP packets with a different packetization rate than the rate used for sending.

Any Media Endpoint that originates and/or terminates voice traffic **MUST** support the [\[ITU-T G.711\]](#) μ -Law and A-Law PCM codecs with a packetization rate of 20 ms. Any device intended for low-bandwidth operation **SHOULD** support [\[ITU-T G.729\]](#) codecs with a packetization rate of 20 ms.

In the absence of a specific indication that receiving G.711 discontinuously using the Comfort Noise (CN) payload type defined in [\[RFC 3389\]](#) is supported, the SIP-PBX or SP-SSE **MUST** assume that the far end Media Endpoint does not support receiving G.711 discontinuously. In order to indicate in SDP that receiving G.711 discontinuously is supported by the local Media Endpoint, the SIP-PBX/SP-SSE **MUST** include payload type 13 in the "m=audio" line as described in [\[RFC 3389\]](#).

It is possible that the Media Endpoint associated with the Offerer or Answerer supports receiving CN packets but not sending them. In that case, it would be perfectly legal to send SDP with Audio Video Profile (AVP) 13 in the "m=audio" line. The Offerer or Answerer in this case is expressing its Media Endpoint's willingness to receive CN packets even if its Media Endpoint never sends any itself.

In the absence of a specific indication that receiving G.729 discontinuously (i.e., [\[ITU-T G.729\]](#) Annex B) is not supported, the SP-SSE/SIP-PBX **MUST** assume that the far end Media Endpoint supports receiving G.729 discontinuously. In order to indicate in SDP that receiving G.729 discontinuously is not supported by the local Media Endpoint, the "a=fmtp:18 annexb=no" attribute **MUST** be included. See Section 2.1.9 in [\[RFC 4856\]](#).

It is possible that the Media Endpoint associated with the Offerer or Answerer supports receiving [\[ITU-T G.729\]](#) Annex B but not sending it. In that case, it would be perfectly legal to send SDP with "annexb=yes" (or without any parameter since that means the same thing). The Offerer or Answerer in this case is expressing its Media Endpoint's willingness to receive [\[ITU-T G.729\]](#) Annex B packets, even if the local Media Endpoint never sends any itself.

14.3 *Transport of DTMF Tones*

A SP-SSE/SIP-PBX **MUST** advertize support for telephone-events [[RFC 4733](#)] in its SDP on behalf of any Media Endpoint that supports receiving DTMF digits using [[RFC 4733](#)] procedures.

Any Media Endpoint that supports receiving DTMF **MUST** support [[RFC 4733](#)] procedures.

Any Media Endpoint that supports sending DTMF **MUST** use the [[RFC 4733](#)] procedures to transmit DTMF tones using the RTP telephone-event payload format, provided that the other side has advertized support for receiving [[RFC 4733](#)] in the offer/answer exchange.

For any local Media Endpoint that supports receiving telephone-event packets, the SIP-PBX or SP-SSE **MUST** include the supported events in an "a=fmtp:" line as is described as mandatory in [[RFC 4733](#)].

To provide backward compatibility with [[RFC 2833](#)] implementations, any Media Endpoint **MUST** be prepared to receive telephone-event packets for all events in the range 0-15 and a SIP-PBX or SP-SSE **MUST** be prepared to accept SDP with a payload type mapped to telephone-event, even if it does not have an associated "a=fmtp" line.

14.4 *Echo Cancellation*

Any Media Endpoint that can introduce echo **MUST** provide [[ITU-T G.168](#)]-compliant echo cancellation.

14.5 *FAX Calls*

In-band fax transmissions are especially problematic over packet networks, especially for calls that traverse the public Internet or other network that doesn't offer adequate QOS.

Media Endpoints that support fax (e.g., a SIP media server that can originate/terminate faxes) and Media Endpoints that can act as a T.30 gateway (e.g., a Media Endpoint that supports an RJ11 analog telephone interface) **MUST** support the [[ITU-T T.38](#)] Recommendation.

Media Endpoints that support [[ITU-T T.38](#)] **MUST** support User Datagram Protocol Transport Layer (UDPTL) transport.

14.6 *Call Progress Tones*

Media Endpoints **SHOULD** locally generate call progress tones or announcements, or other suitable indications, when the response to an INVITE request indicates call failure. Selection of the particular tone or announcement for a given response code might depend on local practices and regulation, but otherwise is left to the equipment manufacturer's discretion.

14.7 Ringback Tone and Early Media

The delivery of in-band announcements and call progress tones from the Service Provider to a caller before a call is answered is achieved through early media.

When acting as a call originator, the SIP-PBX, upon receipt of a 180 provisional response message (whether reliable [\[RFC 3262\]](#) or unreliable) **MUST** instruct the Media Endpoint to play local ringback tone to the user. Upon receipt of SDP in any 18x provisional response message (reliable [\[RFC 3262\]](#) or unreliable), the SIP-PBX **MUST** forward this information to the Media Endpoint.

When acting as a call terminator and expecting the originating end to provide local ringback tone, the Media Endpoint **MUST NOT** send RTP packets to the originator if a 180 provisional response message was sent.

A Media Endpoint, on receipt of an instruction to play local ringback tone, **MUST** do so until it receives valid RTP packets or is instructed by the SIP-PBX that the call has been answered. On receipt of valid RTP packets, a Media Endpoint **MUST** disable any local ringback tone and play the received media. A Media Endpoint, on receipt of information concerning received SDP, **MAY** use the information to determine whether RTP packets received are valid and **MAY** discard RTP packets arriving before that time.

14.8 Putting a Session on Hold

A 2-way session can be put on hold by using an offer-answer exchange (Section 14.1) and the directionality attributes as described below.

When the hold initiator (which may be the SIP-PBX or SP-SSE acting transparently as Media Endpoint) provides music-on-hold (MOH) treatment:

- The MOH source in the SP-SSE/SIP-PBX is based on local policy.
- The hold initiator **MUST** set the SDP directionality attribute to "a=sendonly".

If the hold initiator does not provide MOH, it **MUST** set the SDP directionality attribute to "a=inactive" or "a=sendonly". The attribute "a=inactive" is **RECOMMENDED** because it provides an indication to the held entity that MOH is not being provided by the hold initiator.

A SP-SSE/SIP-PBX **MUST** support the ability to receive SDP session descriptions that have the 'c=' field set to all zeros (0.0.0.0), when the addrtpe field is IPV4. Note that this is for support of non-compliant remote SIP signaling entities that use this deprecated syntax from RFC 2543, rather than the "a=sendonly" or "a=inactive" syntax specified in [\[RFC 3264\]](#).

15 Annex A: Registration Mode

As stated in Section 7, in Registration mode, the SIP-PBX conveys its SIP signaling address to the Service Provider Network using the SIP registration procedure. In effect, the SIP-PBX registers with the Service Provider Network, just as a directly hosted SIP endpoint would register. However, because a SIP-PBX has multiple Enterprise Public Identities, it needs to register a contact address on behalf of each of these. Rather than performing a separate registration procedure for each Enterprise Public Identity, Registration mode makes use of the mechanism in [\[RFC 6140\]](#) to achieve multiple registrations using a single REGISTER transaction.

According to this mechanism, the SIP-PBX delivers to the SP-SSE in the "Contact" header field of a REGISTER request a template from which the SP-SSE can construct contact URIs for each of the AORs (Enterprise Public Identities) assigned to the SIP-PBX, and thus can register these contact URIs within its location service. These registered contact URIs can then be used to deliver to the SIP-PBX inbound requests targeted at the AORs concerned. The mechanism can be used with AORs comprising SIP URIs based on global E.164 numbers and the Service Provider's domain name or sub-domain name. This is consistent with requirements for Enterprise Public Identities for Registration mode in Section 9.

As a pre-requisite, the SIP-PBX and the SP-SSE need to be provisioned with the set of E.164 numbers (and hence the set of Enterprise Public Identities) assigned to the SIP-PBX and with a Registration AOR for use in the "To" header field of the REGISTER request. The SIP-PBX **MUST** be capable of provisioning any format of SIP-URI as the Registration AOR, in order to accommodate SP-SSE requirements (i.e., the Registration AOR is not subject to the same constraints as Enterprise Public Identities and could, for example, be an "email-style" SIP URI).

The requirements of this section apply only to SIP-PBXs and SP-SSEs that support Registration mode.

15.1 Locating SIP Servers

15.1.1 Enterprise Requirements

The SIP-PBX **MUST** provide its SIP signaling address(es) and port(s) to the SP-SSE using the SIP registration procedure described in Section 15.4.

The SIP-PBX **MUST** be capable of obtaining information about the SP-SSE, using the procedure described in Section 16.1.1.2.

15.1.2 Service Provider Network Requirements

The SP-SSE **MUST** make its SIP signaling address(es) and port(s) available to the Enterprise Network as specified in Section 16.1.2.1.

The SP-SSE **MUST** obtain the SIP-PBX signaling address/port using SIP registration, as described in Section 15.4.

15.2 Signaling Security

In Registration mode, the following rules for using TLS apply:

- Both SIP-PBX and SP-SSE **MUST** support the TLS Server Authentication model, whereby the SP-SSE (acting as TLS server), provides its certificate to the SIP-PBX (acting as TLS client) as part of the TLS establishment phase. Note that this is essentially the same model as secure TLS/SSL connections on the Public Internet for HTTP. This avoids the need for the SIP-PBX to have a certificate. However, a consequence is that the SIP-PBX must initiate the TLS session (in order to act as the TLS client).
- The SIP-PBX **MUST** be capable of initiating the establishment of a TLS session.
- The SIP-PBX **MUST** be capable of being provisioned with either a certification authority certificate or with a copy of the certificate the SP-SSE plans to use (or a fingerprint thereof). However, the SIP-PBX does not need to be provisioned with a certificate.
- The SIP-PBX **MUST** validate the certificate received during TLS establishment using the path validation procedure described in [\[RFC 5280\]](#).
- The SIP-PBX **SHOULD** verify the status of the certificate received during TLS establishment. Status verification steps include checking the status of all certificates in the chain using certificate revocation lists (CRLs) [\[RFC 5280\]](#) or Online Certificate Status Protocol (OCSP) [\[RFC 2560\]](#).
- The SIP-PBX **MUST** be capable of being configured to require use of TLS to initiate a session. When TLS is configured as required for session initiation, a SIP-PBX **MUST NOT** initiate sessions with other transports (UDP or TCP), even if the SP-SSE indicates that these are available via DNS NAPTR and/or SRV resource records.

In Registration mode, when the SIP-PBX is configured to require use of TLS with an SP-SSE, the following requirements apply:

- The SIP-PBX **MUST** initiate the establishment of the TLS session.
- The SIP-PBX **MUST NOT** utilize other transports (UDP or TCP), even if the SP-SSE indicates that these are available via configuration of DNS NAPTR and/or SRV resource records.

When the SP-SSE is configured to accept TLS connections, the following requirements apply:

- When configuring DNS NAPTR and/or SRV resource records in accordance with Section 15.1.2, the SP-SSE **SHOULD** indicate support for TLS.
- The SP-SSE **MUST** be configured with a verifiable digital certificate to secure a TLS session.
- The SP-SSE **MUST** use certificates that are signed by a third party certification authority unless the certificates can be validated through some other means, such as being pre-installed at the SIP-PBX or signed by the SP-SSE itself.

When using TLS (as a result of being configured to require use of TLS, or as a result of discovering the availability of TLS from DNS), the SIP-PBX **MUST** establish a TLS connection (if not already established) prior to registration and **MUST** use that connection to deliver the REGISTER request and all subsequent SIP messages to the SP-SSE. The SP-SSE **MUST** authenticate the SIP-PBX using SIP digest authentication, as specified in Section 15.4, and reject the REGISTER request if authentication fails. Following successful registration, the SP-SSE **MUST** use a TLS connection that is authenticated as a connection to this SIP-PBX to deliver all SIP requests to the SIP-PBX.

The SIP-PBX and the SP-SSE **MUST** avoid closing down the TLS connection, other than in exceptional circumstances (e.g., for maintenance). The SIP-PBX is responsible for attempting to keep the connection alive, and if the TLS connection fails, the SIP-PBX is responsible for re-establishing the TLS connection at the earliest opportunity and registering again, in order that the SP-SSE can deliver SIP requests to the SIP-PBX at any time (e.g., in support of incoming calls).

15.2.1 The use of transport=tls parameter

When a SIP-PBX registers, the SP-SSE **MUST** ignore the transport=tls parameter in the "Contact" header field URI.

The reachability through TLS is indirectly determined by the SP-SSE because the registration itself is using TLS.

15.3 Firewall and NAT Traversal

Any IP addresses contained within the header fields and message body parts (e.g. SDP) of SIP messages exchanged between the Service Provider and Enterprise Networks **MUST** be publicly routable addresses, unless the Service Provider Network is providing an implicit NAT traversal function or the two are using a private VPN-style address space.

15.4 Registration

The SIP-PBX and SP-SSE **MUST** support multiple AOR registration in accordance with [\[RFC 6140\]](#), using the provisioned Registration AOR and the set of provisioned Enterprise Public Identities, even if there is only a single provisioned Enterprise Public Identity.

In the REGISTER request, the SIP-PBX **MUST** include a Contact URI in accordance with [\[RFC 6140\]](#) using a suitable domain part, e.g., the SIP-PBX's IP address. The SIP-PBX **MUST** insert the Registration AOR in the "From" and "To" header fields of the REGISTER request.

The SIP-PBX and SP-SSE **MUST** support the authentication mechanisms outlined in Section 15.6 for digest authentication for the REGISTER requests, using a user name and password agreed to by both parties.

15.4.1 Registration Failures

This section details the behavior requirements for the SP-SSE and SIP-PBX for Registration failure scenarios.

15.4.1.1 *Failure of SIP-PBX to reach the SP-SSE*

If the SIP-PBX fails to receive any response to a REGISTER request in Timer_F time (typically 32 seconds) or encounters a transport error when sending a REGISTER request, the SIP-PBX **MUST** consider the SP-SSE unreachable and try to register with an alternate SP-SSE address if it has one. If the SIP-PBX has an established connection-based transport (e.g., TCP) to the SP-SSE, and Timer_F expires or a transport error is encountered as above, it **MUST** try to re-establish a connection to the same SP-SSE before considering it unreachable, by resetting Timer_F and sending a new REGISTER request. The SIP-PBX **MUST NOT** attempt to re-establish the connection to the same SP-SSE more than once before considering the SP-SSE unreachable. This allows for cases where the SP-SSE lost previous transport connection state but is otherwise reachable, such that the SIP-PBX will try a second time and only consider the SP-SSE unreachable if that second attempt fails.

If no SP-SSE is reachable, or no alternates are available, the SIP-PBX **MUST** delay reattempting Registration for 30 seconds, and increasing this delay value by doubling it for each successive delivery failure until delivery succeeds, up to a maximum value of 960 seconds.

Note that receiving an explicit non-2xx final response from the SP-SSE does not constitute a delivery failure. Instead, behaviors for such final responses are noted in the following sections.

15.4.1.2 *Redirection of SIP-PBX from SP-SSE*

The SP-SSE **MUST NOT** issue a 302 Moved Temporarily redirect response to a REGISTER request, to get the SIP-PBX to Register with an alternate SP-SSE address identified by the Contact URI in the response.

15.4.1.3 *Unknown SIP-PBX Identity*

The SP-SSE **MUST** issue a 404 Not Found response to a REGISTER request, if the Registration AOR of the SIP-PBX is not found in its database. An SIP-PBX receiving such a response to a REGISTER request **MUST** consider the Registration attempt to have failed, and notify the SIP-PBX administrator if possible through some means. The SIP-PBX **SHOULD** follow the backoff procedures defined previously in Section 15.4.1.1.

15.4.1.4 Incorrect SIP-PBX Password

If the digest challenge response of the SIP-PBX in its REGISTER request is stale or invalid, the SP-SSE **MUST** issue one of the following response codes:

- a 401 Unauthorized,
- a 407 Proxy Authentication Required or
- a 403 Forbidden

unless the SP-SSE is configured to silently discard these requests based on policy.

If a SIP-PBX receives more than three responses of 401, 407 or 403 in aggregate, without a different response other than one of those in between, then the SIP-PBX **MUST** consider the Registration attempt to have failed, and notify the SIP-PBX administrator if possible through some means. The SIP-PBX **SHOULD** follow the backoff procedures defined previously in Section 15.4.1.1.

15.4.1.5 Other servers unreachable from SP-SSE

If an SP-SSE is unable to complete registration, it **MAY** issue a 480 Temporarily Unavailable response code for a REGISTER request. An SIP-PBX receiving such a response to a REGISTER request **MUST** act exactly as if delivery to the SP-SSE had failed per Section 15.4.1.1, and **MUST** follow the backoff procedures defined previously in Section 15.4.1.1.

15.4.1.6 SP-SSE Administratively Disabled or Overloaded

An overloaded SP-SSE **MUST** generate a 503 Service Unavailable or 500 Internal Error response code to a REGISTER request, unless it is silently discarding requests due to overload, and **SHOULD** include a "Retry-After" header field value indicating how long the SIP-PBX should wait before re-attempting a REGISTER request to the same SP-SSE.

This "Retry-After" header field value **SHOULD** include an element of randomness so that all served SIP-PBXes don't become synchronized and repeatedly attempt to register en mass.

A SIP-PBX receiving such a response **MUST** support the "Retry-After" header field, and **MUST** honor the value as follows: if the value is 32 seconds or less, it **MUST** wait the requested time and retry the request to the same SP-SSE; if the value is larger, it **MUST** remember the value for that SP-SSE address instance, and try any alternate SP-SSE addresses it can. If an alternate SP-SSE can be successfully reached and Registration succeeds through the alternate, the SIP-PBX **MAY** discard the "Retry-After" value of the original. Otherwise, it **MUST** wait to reattempt registration to the original SP-SSE for the "Retry-After" interval.

15.4.1.7 *Other 4xx/5xx/6xx Responses*

Any 4xx, 5xx or 6xx-class response to a REGISTER request not explicitly identified above **SHOULD** be treated in a similar manner as Section 15.4.1.1 unless it can automatically be resolved by the SIP-PBX internally - i.e., unless it is part of an explicit negotiation mechanism or procedure. It **SHOULD** be treated as a delivery failure with a maximum retry interval of 960 seconds (16 minutes), unless a longer "Retry-After" header field is specified.

15.4.2 Registration-related failures for other requests

If a SIP-PBX encounters a transport error when attempting to contact the SP-SSE, encounters Timer F expiry (non-INVITE requests) or Timer B expiry (INVITE requests), or receives a 403 response for any non-REGISTER request, the SIP-PBX **MUST**

- consider the request attempt to have failed,
- assume that the SIP-PBX's registration is no longer active at the SP-SSE, and
- notify the SIP-PBX administrator if possible through some means.

The SIP-PBX **SHOULD** attempt re-registration using the procedures defined previously in Section 15.4.1.1.

15.5 *Maintaining Registration*

It is important that registrations are maintained and, in the event of failure, are re-established quickly, since the SP-SSE depends on the SIP-PBX being registered in order to deliver inbound requests to the SIP-PBX. Where TCP (with or without TLS) is used, the TCP connection needs to be maintained as the means for delivering inbound requests.

Because NATs and firewalls may drop a TCP connection through lack of use, measures need to be taken to keep the connection alive and detect whether it has been dropped. Similarly, where UDP is used, it is necessary to keep the path through NATs and firewalls alive. Therefore the SIP-PBX **MUST** honor the REGISTER expiry time provided by the SP-SSE, and **MAY** send REGISTER requests more frequently if NAT and firewall policies require this.

If failure is detected a SIP-PBX **MUST** attempt reconnection, and if that fails **MUST** try an alternative SP-SSE if available, in accordance with Section 15.4.1.1.

15.6 *Authentication*

15.6.1 Authentication of the Enterprise by the Service Provider

The SP-SSE authenticates the SIP-PBX using SIP Digest authentication mechanism.

The SIP-PBX and SP-SSE **MUST** support the digest authentication scheme as described in Section 22.4 of [\[RFC 3261\]](#). The Service Provider assigns the SIP-PBX a username and associated password that are valid within the Service Provider's domain (realm).

The following rules apply:

1. The SP-SSE may challenge any SIP request. The SIP-PBX **MUST** support receiving 401 Unauthorized and 407 Proxy Authentication Required from the SP-SSE. When so challenged by the SP-SSE, the SIP-PBX **MUST** respond with authentication credentials that are valid within the Service Provider's realm (i.e. based on the username and password supplied by the Service Provider).
2. In order to avoid unnecessary challenges, the SIP-PBX **SHOULD** include its authentication credentials using the current nonce in each subsequent request that allows authentication credentials to be sent to the SP-SSE.

When Digest Authentication is used over a path that is not protected by TLS, the credentials used are subject to offline "dictionary attacks", and successful attackers can then make calls that are billed to the SIP-PBX. Credentials provided to the SIP-PBX should be selected with this threat in mind. For example, passwords that appear in dictionaries would be poor choices. The credentials used for Digest Authentication should be machine-generated to have at least 64 bits of cryptographic randomness and then delivered via an automated provisioning mechanism. Human-memorable passwords are not the best choices. Since no end user has to enter one of these passwords, it is practical to use strong credentials.

15.6.2 Authentication of the Service Provider by the Enterprise

Authentication of the Service Provider by the Enterprise is supported using TLS server authentication. If TLS is required (based on local configuration data), then the SIP-PBX **MUST** perform TLS server authentication as described in Section 15.2.

15.6.3 Accounting

Accounting places no special requirements on the SIPconnect 1.1 interface. The SP-SSE may generate billing records for calls originating from the SIP-PBX, based on the local policy of the Service Provider. The SIP-PBX is not required to signal a billing number to the SP-SSE (i.e., the SP-SSE will be configured with the billing number associated with billable incoming calls from the SIP-PBX).

15.7 Routing Inbound Requests to the SIP-PBX

The SP-SSE **MUST** route inbound out-of-dialog requests targeted at Enterprise Public Identities to the registered SIP-PBX in accordance with [\[RFC 6140\]](#). This means that the Request-URI will comprise a SIP-URI containing the user part of the target Enterprise Public Identity and the domain part of the registered contact for that AOR.

16 Annex B: Static Mode

In the Static mode, the Service Provider and Enterprise Networks view each other as peer networks. The SP-SSE is configured with the domain name of the Enterprise and is either configured with the static IP address of the SIP-PBX or obtains the IP address of the SIP-PBX via DNS.

16.1 Locating SIP Servers

16.1.1 Enterprise Requirements

16.1.1.1 Providing Enterprise Address to SP-SSE

The SIP-PBX **MUST** provide its SIP signaling address and port to the SP-SSE using one of the following mechanisms:

- DNS: The Enterprise Network ensures the existence of a publicly-accessible DNS server that is authoritative for its domain (or a sub-domain delegated by the Service Provider for use by the Enterprise). This DNS server **SHOULD** provide a DNS interface that supports NAPTR resource records and **MUST** provide a DNS interface that supports SRV resource records [[RFC 2782](#)].
- Configuration: The Enterprise Network provides information to allow the Service Provider to configure mapping of the Enterprise Fully Qualified Domain Name (FQDN) to the SIP-PBX signaling address/port and transport at the SP-SSE.

16.1.1.2 Obtaining SP-SSE Address

Except when a TLS connection already exists, the SIP-PBX **MUST** use one of the following mechanisms to obtain the address and port of the SP-SSE and the transport protocol (UDP, TCP or TLS) to be used:

- [[RFC 3263](#)] "Locating SIP Servers": SIP-PBX utilizes DNS NAPTR and SRV queries as described in [[RFC 3263](#)] to determine the IP address(es), transport protocol(s), and port number(s) of the SP-SSE(s) associated with the Service Provider's domain name. This option assumes that the SIP-PBX has been pre-configured with the domain name of the Service Provider Network.
- Configuration: One or more transport protocols and SIP signaling address(es)/port(s) of the SP-SSE are configured in the SIP-PBX. A configured SP-SSE signaling address **SHOULD** be in the form of a hostname that can be resolved through DNS A/AAAA resource records, rather than an IP address (see additional guidance in Section 17.1).

When a TLS connection already exists, the SIP-PBX **MUST** reuse that TLS connection for all SIP messages.

16.1.2 Service Provider Network Requirements

16.1.2.1 *Providing SP-SSE Address to Enterprise*

The SP-SSE **MUST** be reachable through a publicly-accessible DNS server. The DNS server **SHOULD** provide a DNS interface that supports NAPTR resource records and **MUST** provide a DNS interface that supports SRV resource records.

Though not required, it is **RECOMMENDED** that Service Providers provide redundant SIP Signaling addresses.

16.1.2.2 *Obtaining the Enterprise Network Address*

The SP-SSE **MUST** support both of the following mechanisms to obtain the address and port of the SIP-PBX and the transport protocol (UDP, TCP or TLS) to be used and, except when a TLS connection already exists, **MUST** use one of these mechanisms:

- DNS: SP-SSE utilizes DNS NAPTR and SRV queries for the pre-configured domain name of the Enterprise Network, as described in [[RFC 3263](#)], to determine the IP address, transport protocol, and port number of the SIP-PBX(s) associated with the Enterprise Network's domain name.
- Configuration: The mapping of the Enterprise FQDN to the SIP-PBX signaling address/port and transport protocol is statically configured in the SP-SSE. A configured SIP-PBX signaling address **SHOULD** be in the form of a hostname that can be resolved through DNS A/AAAA resource records, rather than an IP address (see additional guidance in Section 17.1).

When a TLS connection already exists, the SP-SSE **MUST** reuse that TLS connection for all SIP messages.

16.2 *Signaling Security*

The following requirements for using TLS apply to SIP-PBX and SP-SSE implementations supporting Static mode:

- Both SIP-PBX and SP-SSE **MUST** support the TLS Mutual Authentication model, whereby both the SP-SSE and the SIP-PBX provide their respective certificate as part of the TLS establishment phase.
- Both SIP-PBX and SP-SSE **MUST** be able to initiate the establishment of a TLS session.
- Both SIP-PBX and SP-SSE **MUST** be capable of being provisioned with either a certification authority certificate or with a copy of the certificate the peer SIP endpoint plans to use (or a fingerprint thereof).
- Both SIP-PBX and SP-SSE **MUST** validate the certificate received during TLS establishment using the path validation procedure described in [[RFC 5280](#)].

- Both SIP-PBX and SP-SSE **SHOULD** verify the status of the certificate received during TLS establishment. Status verification steps include checking the status of all certificates in the chain using certificate revocation lists (CRLs) [[RFC 5280](#)] or Online Certificate Status Protocol (OCSP) [[RFC 2560](#)].
- Both SIP-PBX and SP-SSE **MUST** be capable of being configured to require use of TLS to initiate a session to a particular peer. When TLS is configured to be required for session initiation to a peer, a SIP-PBX or SP-SSE **MUST NOT** initiate sessions with other transports (UDP or TCP), even if the peer indicates that these are available via configuration of DNS NAPTR and/or SRV resource records.
- Both SIP-PBX and SP-SSE **MUST** be capable of being configured to require use of TLS to accept sessions initiated to it by a peer. When TLS is configured to be required to accept sessions initiated from all peers, a SIP-PBX **MUST NOT** advertise support for other transports (UDP or TCP), via configuration of DNS NAPTR and/or SRV resource records.

When a SIP-PBX is configured to accept TLS connections, the following requirements apply:

- When configuring DNS NAPTR and/or SRV resource records in accordance with Section 16.1.1.1, the SIP-PBX **SHOULD** indicate support for TLS.
- The SIP-PBX **MUST** be configured with a verifiable digital certificate to secure a TLS session.
- The SIP-PBX **MUST** be configured with a certificate signed by a third party certification authority unless the configured certificate can be validated through some other means, such as being pre-installed on the SP-SSE or signed by the SIP-PBX itself.

When an SP-SSE is configured to accept TLS connections, the following requirements apply:

- When configuring DNS NAPTR and/or SRV resource records in accordance with Section 16.1.2.1, the SP-SSE **SHOULD** indicate support for TLS.
- The SP-SSE **MUST** be configured with a verifiable digital certificate to secure a TLS session.
- The SP-SSE **MUST** be configured with a certificate signed by a third party certification authority unless the configured certificate can be validated through some other means, such as being pre-installed on the SIP-PBX or signed by the SP-SSE itself.

Although not essential, it is good practice to keep a TLS connection alive and to re-use it for messages in either direction, to avoid unnecessary processing and delays in establishing a new connection for each message or transaction.

16.3 Firewall and NAT Traversal

The same considerations described for Registration mode in Section 15.3 apply here.

In addition, Static mode requires that both the SIP-PBX and the SP-SSE be directly reachable, which may require configuration of a static binding if NATs or firewalls are present between those elements.

16.4 *Failover and Recovery*

SIP-PBXes that require timely detection of SIP peer failure **MAY** use any of these mechanisms as keep-alives:

- Sending an OPTIONS request periodically, or
- Sending a carriage return/line feed periodically (TCP only – Note: this is a unidirectional CR/LF with no application layer acknowledgement. This can generate TCP resets if the SIP peer fails).

SIP-PBXes that support one of these mechanisms **MUST** also support a mechanism that allows the keep-alive interval to be configured.

16.5 *Authentication*

The SP-SSE and SIP-PBX authenticate each other using TLS mutual authentication. If TLS is required (based on local configuration data), then the SP-SSE and SIP-PBX **MUST** perform TLS mutual authentication as described in Section 16.2.

16.6 *Routing Inbound Requests to the SIP-PBX*

The SP-SSE **MUST** populate the Request-URI of the INVITE request with the Enterprise Public Identity of the called Enterprise user in the valid form defined in Section 9, or with a Contact URI provided by the SIP PBX in a previous request or response.

17 Appendix: Topics Not Addressed in SIPconnect 1.1

There are several topics that came up during discussions on SIPconnect 1.1 that the SIP Forum expects to deal with in the next version of the Technical Recommendation, but were not ready for inclusion in version 1.1. This section is intended for network planners who expect to track SIPconnect as it evolves.

17.1 *IPv6*

The SIP Forum recognizes the eventual depletion of IPv4 addresses is looming. However, the SIP Forum also recognizes that at the time of publication of SIPconnect 1.1, IPv6 is not ubiquitously implemented or deployed. Therefore, the SIP Forum was unable to mandate IPv6 support for either the SIP-PBX or the SP-SSE.

Instead the SIP Forum was able to publish guidelines so the transition to IPv6 occurs with the least impact on compliant SIPconnect 1.1 implementations. These guidelines are as follows.

- Do not hard-code IP addresses in configuration files (other than configuration files used by DHCP). Use DNS instead.
- Expect IPv6 addresses whenever one receives an IP address in a message. By "message", we mean not only SIP and SDP messages, but also DNS, HTTP, TLS, and so on.

SIPconnect 1.1 does not mandate the use of explicit IPv4 addresses. Rather, SIPconnect 1.1 suggests using hostnames and fully qualified domain names to allow support for IPv4 and IPv6. The use of statically configured IPv4 or IPv6 addresses by SIP-PBXs and SP-SSEs is compliant to this Technical Recommendation, but will make interoperability with heterogeneous SIP Service Providers and Enterprise Networks more difficult.

A SIPconnect 1.1 SIP-PBX and a SIPconnect 1.1 SP-SSE that both implement the same IP version (either IPv4 or IPv6) should interoperate over their respective IP networks. IPv6-unaware SIP-PBXs and SP-SSEs will only be able to support IPv4-unaware SP-SSEs and SIP-PBXs respectively if an IETF transition mechanism is in place on the network and statically configured IP addresses are not used.

On February 3, 2011, the Internet Assigned Numbering Authority (IANA) allocated the last five "/8" IPv4 address blocks to the Regional Internet Registries. In light of the imminent exhaustion of IPv4 address space, future versions of the SIPconnect Technical Recommendation will almost certainly mandate support for IPv6.

17.2 UDP

Although most of our deployment experience has been with SIP over UDP transport, a number of recent protocol extensions increase the size of SIP requests and/or responses. While each of these extensions, taken in isolation, may not increase the size of a request or response beyond the Maximum Transmission Unit (MTU) size, when taken together, they increase the likelihood of fragmentation when using UDP transport.

We recognize that UDP is still widely deployed, so we continued to allow SIP over UDP as an optional mode of operation in order to accommodate legacy devices, but we expect to remove SIP over UDP as an optional mode of operation in the next version of SIPconnect. SIP over TCP is already the preferred form of operation in SIPconnect 1.1, and is already mandatory-to-implement.

Even in SIPconnect 1.1, planners for deployments should carefully consider whether they expect to use SIP or SDP extensions that could result in SIP requests or responses exceeding the maximum MTU size, and consequently encounter IP-level fragmentation of UDP packets carrying these requests and responses.

17.3 Emergency Services

We had expected to require support for the "sos" service URN tree in order to provide emergency services [RFC 5031] in SIPconnect 1.1, but we don't have enough deployment experience with this mechanism to require SP-SSEs and SIP-PBXes to add support for a new technique for accomplishing such a critical service.

We expect that SIP-PBXes and SP-SSEs will continue to use nation-specific dial strings to invoke emergency services in the SIPconnect 1.1 timeframe.

One can expect future versions of the SIPconnect Technical Recommendation to mandate support for "sos" service URN tree support on both the SIP-PBX and SP-SSE.

17.4 FAX Over IP

We recognize that Fax operation over SIP networks represents a unique challenge for network operators. Since the release of SIPconnect 1.0, a number of issues have been documented that affect the reliability of fax over SIP networks.

The SIP Forum Fax-over-IP (FoIP) Interoperability Task Group has published Version 1.0 of its official Problem Statement, available on the SIP Forum website at http://www.sipforum.org/component/option,com_docman/task,doc_download/gid,303/Itemid,261/. The Problem Statement details the various interoperability issues that been identified as affecting FoIP services.

Work and research is ongoing. The SIP Forum hopes to provide additional guidance in future versions of SIPconnect based on the work of the FoIP Interoperability Task Group.

17.5 Service Provider-hosted Voice Mail

We had hoped to make recommendations about Service Provider-hosted Voice Mail in SIPconnect 1.1, but we identified at least three different mechanisms that have been deployed (the Voice Mail URI, the "Diversion" header field, and the "History-Info" header field).

All three mechanisms have difficulties, and none are deployed ubiquitously, so we were unable to come to consensus on which of these to recommend in SIPconnect 1.1. We are unable to point to a revised History-Info mechanism, which addresses problems with the existing mechanism, because it's still under development in the IETF,

We will revisit this topic when the IETF completes its History-Info revision, and hope to provide guidance in future versions of SIPConnect.

References

ITU-T E.164 International Telecommunications Union, "Recommendation E.164: The international public telecommunication numbering plan", May 1997, <<http://www.itu.int>>.

ITU-T G.168 International Telecommunications Union, "Recommendation G.168: Digital network echo cancellers", January 2007, <<http://www.itu.int>>.

ITU-T G.711 International Telecommunications Union, "Recommendation G.711: Pulse code modulation (PCM) of voice frequencies ", November 1988, <<http://www.itu.int>>.

ITU-T G.729 International Telecommunications Union, "Recommendation ITU-T G.729: Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)", January 2007, <<http://www.itu.int>>.

ITU-T T.38 International Telecommunications Union, "Recommendation T.38: Procedures for real-time Group 3 facsimile communication over IP networks ", April 2007, <<http://www.itu.int/rec/T-REC-T.38/e>>.

RFC 2119 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

RFC 2246 T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

RFC 2560 M. Myers et. al., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", RFC 2560, June 1999.

RFC 2782 A. Gulbrandsen, P. Vixie, L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

RFC 2833 H. Schulzrinne, S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", RFC 2833, May 2000.

RFC 3261 Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

RFC 3262 J. Rosenberg, H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

RFC 3263 J. Rosenberg, H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

- RFC 3264 J. Rosenberg, H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.
- RFC 3265 A. B. Roach, "Session Initiation Protocol (SIP)-Specific Event Notification. RFC 3265, June 2002.
- RFC 3311 J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, September 2002.
- RFC 3323 J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.
- RFC 3325 C. Jennings, J. Peterson, M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.
- RFC 3327 D. Willis, and B. Hoeneisen "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", RFC 3327, December 2002.
- RFC 3515 R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.
- RFC 3550 H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, July 2003.
- RFC 3389 R. Zopf, "Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)", RFC 3389, September 2002.
- RFC 4538 J. Rosenberg, "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)", RFC 4538, June 2006.
- RFC 4566 M. Handley, V. Jacobson, C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.
- RFC 4733 H. Schulzrinne, T. Taylor, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals", RFC 4733 (Obsoletes RFC 2833), December 2006.
- RFC 4856 S. Casner, "Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences", RFC 4856, March 2007.
- RFC 4967 B. Rosen, "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier", RFC 4967, July 2007.
- RFC 5031 H. Schulzrinne, "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.

RFC 5280 D. Cooper et. al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2009.

RFC 5589 R. Sparks, A. Johnston, D. Petrie, "Session Initiation Protocol Call Control – Transfer", RFC 5589, March 2009.

RFC 5806 S. Levy, M. Mohali, "Diversion Indication in SIP", RFC 5806, March 2010.

RFC 5876 J. Elwell, "Updates to Asserted Identity in the Session Initiation Protocol (SIP)", RFC 5876, April 2010.

RFC 6140 A. B. Roach, "Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)", RFC 6140, March 2011.

18 Acknowledgements for SIPconnect 1.1 Initial Contributions

The SIP Forum Technical Working Group chairs requested contributions of suggested revisions to SIPconnect 1.0 in order to kick-start SIPconnect 1.1 work, and selected CableLabs' contribution as a starting point for SIPconnect 1.1. The editor also included text and suggestions from contributions by Avaya, Broadsoft, Cbeyond, Microsoft, and Siemens in the initial (v00) draft. The editor thanks each of these contributors for their assistance.

19 Contributors to SIPconnect 1.1 and Contact Information

Bernard Aboba
Microsoft Corporation
E-mail: Bernard_Aboba@hotmail.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

François Audet
Skype Labs
E-mail: francois.audet@skypelabs.com

Shaun Bharrat
Sonus Networks
E-mail: sbharrat@sonusnet.com

Eric Burger
Georgetown University
E-mail: eburger@sipforum.org
<http://www.standardstrack.com>

Spencer Dawkins
Huawei Technologies (USA)
E-mail: spencer@wonderhamster.org

John Elwell
Siemens Enterprise Communications
E-mail: john.elwell@Siemens-enterprise.com

Alan Johnston
Avaya
E-mail: abjohnston@avaya.com

David Hancock
CableLabs
E-mail: d.hancock@cablelabs.com

Cullen Jennings
Cisco
E-mail: fluffy@cisco.com

Hadriel Kaplan
E-mail: hkaplan@acmepacket.com

Brian Lindsay
GENBAND
E-mail: brian.lindsay@genband.com

Richard Shockey
Phone: +1 703.593.2683
E-mail: [richard\(at\)shockey.us](mailto:richard(at)shockey.us)
skype: rshockey101
LinkedIn : www.linkedin.com/in/rshockey101

Mark Stewart
MetaSwitch
E-mail: mark.stewart@metaswitch.com

Theo Zourzouvillys
Skype
E-mail: theo@skype.net

20 Acknowledgements to Contributors to SIPconnect 1.0

SIPconnect 1.1 is a revision of SIPconnect 1.0, so it's appropriate to thank the contributors to SIPconnect 1.0 which formed the basis for this work.

21 Full Copyright Statement

Copyright (C) SIP Forum 2011.

This document is subject to the rights, licenses and restrictions contained in SIP Forum Recommendation [sf-admin-copyrightpolicy-v.1.0], and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF

ANY), THE SIP FORUM DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

REQUEST FOR PROPOSAL FOR AN IP-BASED NEXT GENERATION 9-1-1 COMMUNICATION SYSTEM

FOR

Counties of Southern Illinois NG9-1-1 Association

To be submitted by September 21, 2010 to:

Ken Smith - Chairman
300 N. Park Ave.
Herrin, Illinois 62948
618-988-6911

The purpose of this document is to provide interested parties with information to enable them to prepare and submit a proposal for the implementation of an 18-county IP-Based Next Generation 9-1-1 communication system in southern Illinois. CSI originally received and opened bids in December of 2009. Grant applications for this project were denied as we were preparing to select a vendor forcing us to reduce the scope of the project to match the available funding. The association intends to use the results of this process to award a contract for goods and services specified within this RFP. If your proposal has a cost of more than 2.2 million dollars it will not be immediately considered and will be set aside until lower cost alternatives have been explored. Please include your bottom line price on the first page of your response.

We will be providing our own ESInet to connect the originating service providers, PSAPs and data centers. We are seeking bids on the hardware, software and services needed to run a next generation system on that network. We will provide our own CAD systems. We are seeking map display software but not requesting GIS data services. We are also not seeking consulting services. Since this is a national pilot project, CSI would welcome vendor proposals that offer their solutions for free or drastically reduced rates in exchange for the privilege of being selected to lead this unique project.

SECTION I

Project Goals and Objectives

Counties of Southern Illinois NG9-1-1 Association (hereinafter referred to as CSI) is soliciting proposals from qualified and experienced organizations that can provide an IP-Based Next Generation 9-1-1, NENA i3 aligned Communication System. CSI desires to upgrade the aging analog 9-1-1 telephony system with an IP-based solution that meets NENA NG 9-1-1 standards, including the emerging NENA IP-Capable PSAP standards. The desired results will be increased functionality, redundancy, diversity, and scalability. The system must be capable of evolving with NG9-1-1 without requiring additional hardware upgrades and replacements.

This system will be used to process, answer and direct all “calls” placed to 9-1-1. The system must support a minimum of two (2) geographically diverse, fully redundant data/system hosting centers. Our plan is to locate one at the Saline County Sheriff’s Department in Harrisburg and the second at the Jackson County Sheriff’s Department in Murphysboro.

The system should not require a manual switchover and should have automatic failover capability. CSI prefers Common Off the Shelf (COTS) equipment rather than proprietary hardware to enable CSI to lower initial infrastructure cost as well as future hardware replacement costs, and to eliminate costly hardware maintenance contracts.

Vendors must provide the option for CSI to purchase some if not most of its own hardware per specifications supplied by the vendor. The solution should allow for IT personnel from CSI to be trained to provide primary on-site Tier 1 support of the proposed system.

The solution proposed must be capable of receiving 9-1-1 calls in a native Session Internet Protocol (SIP) format upon installation. This would include gateways for legacy wireline, wireless and VOIP calls. Furthermore, the solution proposed must be capable of expansion to multiple additional counties/PSAPs by simply adding additional software and hardware. Systems requiring the replacement of components to expand will not be considered. As an option, we would also consider the additional cost of having administrative calls received in a native SIP format.

The system must be able to integrate with a local ALI database management system as well as an integrated Mapped-ALI display. It is the desire of CSI to have a GIS-centric system that will be able to spatially route calls and the capability to use the GIS database in the future as the primary 9-1-1 validation database.

CSI recognizes that a robust NG9-1-1 communications system capable of accepting all calls for emergency services in an efficient and accurate manner is the primary responsibility of CSI and its members. Reduced system cost, enhanced call taker capability, remote diagnostics and system architecture designed to accept future types of calls are some of the important objectives of this project.

A firm quotation for professional services is being solicited for required services and products in this Request for Proposal (RFP). Required products and services are those that CSI intends to purchase from the successful respondent. All proposal pricing shall be in effect 90 days from the proposal opening date.

This is a complex project involving 28 PSAPs and 18 Emergency Telephone System Boards. It could take longer than the normal 60 days to select a vendor. CSI will consider proposals from firms who plan to share work through a subcontracting agreement. Such proposals will be considered only if one firm assumes the role and all of the responsibilities of a prime contractor. This RFP is soliciting a single quotation. Respondents are encouraged to propose innovative or alternative technical approaches if they will provide technical, schedule, or cost advantages to the project while meeting or exceeding all requirements. Respondents should indicate if they participated in the NENA ICE interoperability testing program. Please indicate how your solution fared in those tests and if it is true I3 or an RFAI solution.

A. Project History

Counties of Southern Illinois is a not for profit association of 18 Emergency Telephone System Boards. For the past three years we have been planning a regional NG 9-1-1 system. We were selected by NENA as a national pilot project to show how an NG solution can be implemented in a rural regional setting. We have received \$695,000 in federal grant money. CSI received proposals in 2009 for a turnkey version of this project anticipating additional federal grants. However, all bids had to be rejected due to cost considerations and for clarification of some NG9-1-1 concepts and standards. CSI has organized as a not-for-profit association. The state legislature has approved a bill that will allow for this regional NG9-1-1 project. That law is attached as exhibit A.

CSI is made up of multiple 911 systems with between one and four PSAPs each. There are a combined 60 positions, with about 40-44 of those manned on any given shift. Please find attached a spreadsheet, (Exhibit B) showing the names, addresses, etc of each PSAP with information concerning their current equipment and other information that will be useful to the vendors.

CSI will be purchasing GIS software both for the PSAPs and the data centers as part of this RFP; however, we have GIS staff that will be maintaining the data layers. We have contracted with SIU-Carbondale, our local university, to provide GIS students to scrub our existing data and put everything in NENA standard formats. Individual 911 Coordinators will provide updates to the road, structure, corporate boundary and jurisdictional layers. We will synchronize the GIS data with the MSAG and ALI databases.

All CSI PSAPs are currently taking phase II wireless calls or will be by the time this project commences.

B. Overview of RFP Structure

The objective of this RFP is to provide sufficient information for qualified respondents to submit written proposals. The RFP is not a contractual offer or commitment to purchase services. Proposals that do not conform to the procedures, format, and content requirements outlined in this RFP will not be considered responsive. Vendors may submit questions to the project manager during the month of August in lieu of holding a pre-proposal meeting that would require extra costs for the vendors.

The RFP contains three sections:

- **Section I** details the project background and time frame.
- **Section II** describes administrative requirements and procedures to be followed in submitting a proposal.
- **Section III** describes the scope of work to be performed and technical specifications.

C. Key Dates

The currently planned dates for the procurement process are:

RFP Release Date	July 21, 2010
Questions due by	August 14, 2010
Proposals Due	September 21, 2010
Vendor presentations	October-November, 2010
Vendor selected	November-December, 2010
Proposed contract award date	January, 2011
Project begins	February 1, 2011

II. Proposal Submission Procedures and Requirements

A. *Proposal Submission*

An original and two (2) copies of your proposal, plus one (1) electronic copy(DVD) must be received no later than 4:00 PM September 21, 2010. Responses should be addressed as follows (mail or express delivery):

Ken Smith CSI Chairman
Williamson Co 911 Office
300 N. Park Ave.
Herrin, Illinois 62948

Proposals may be either mailed or hand delivered; proposals transmitted by FAX machine or other electronic means will ***not*** be accepted. If the proposal is sent by mail, the applicant will be responsible for actual delivery to the proper office before the deadline. Any proposals received after the deadline will be returned unopened. The bids will remain sealed until the bid opening. During the bid opening the proposals will be opened to determine whether a cost and technical proposal have been received with the required copies. The bid opening will be held at CSI headquarters at 9 a.m. on September 10, 2010.

Each proposal must be sealed to provide confidentiality of the information before the submission date and time. CSI will not be responsible for premature opening of proposals not properly labeled. Proposals and presentations should be prepared simply and economically, and give a straightforward and concise description of the Respondent's capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

B. *Requests for Further Information or Clarification*

All respondents should clearly state within their proposals any questions to be addressed by CSI, and identify any assumptions made in formulating the proposals. CSI reserves the right to respond to questions or discuss assumptions made by any Respondent after all proposals have been reviewed.

C. Duly Authorized Signature

The quotation must contain as the first element of the proposal, a cover letter with the signature of a duly authorized officer or agent of the Respondent's company empowered with the right to bind the Respondent. The name and address of the Respondent's designated contact person must also be included. The Respondent shall be fully responsible for all quotation development and submission costs. CSI assumes no contractual obligation as a result of the issuance of this RFP, the preparation or submission of a quotation by a Respondent, the evaluation of an accepted quotation, or the selection of finalists.

1. The Respondent's duly authorized officer or agent shall certify in the proposal's cover letter: A) That his/her quotation is genuine, is not made in the interest of, or on behalf of, any undisclosed person, firm or corporation. B) That (s)he has not directly or indirectly induced or solicited any other Respondent to put in a false or sham bid; C) That (s)he has not solicited or induced any other person, firm, or corporation to refrain from proposing; and D) That (s)he has not sought by collusion to obtain for himself/herself any advantage over any other Respondent or over CSI.
2. Proposals shall be binding upon the Respondent for ninety (90) days from the proposal opening. A Respondent may withdraw or modify his/her quotation any time before the due date by a written request, signed in the same manner by the same person who signed the quote.
3. Provisions of this RFP and the contents of the successful response are considered available for inclusion in final contractual obligations. CSI retains the option of canceling the award if the successful Respondent fails to accept such obligations.

D. Respondent Qualifications

1. Respondents must submit evidence that they have relevant past experience and have previously delivered similar products and services to the ones required.

2. Each Respondent shall be required to show that they have satisfactorily performed similar work in the past and that any claims against such work are disclosed to this agency.

E. Price Proposals

Unless Respondents specifically take exception, prices quoted for work to be performed will be considered firm. In case of error in the extension of prices in the quotation, the unit prices shall govern.

F. Rights Reserved To Customer

Customer reserves the right to:

1. Amend the RFP as necessary and provide revisions.
2. Waive or modify minor irregularities in proposals received, after prior notification to the respondent.
3. Reject any proposal that is incomplete, does not demonstrate the respondent's ability to provide the required services, or which is not responsive to this RFP.
4. Accept the proposal that is, in the sole judgment of CSI most advantageous even though it may not be the lowest priced proposal.
5. Negotiate with any Respondent after proposals are opened, if such action is deemed in the best interest of CSI.
6. Negotiate a contract with another qualified respondent in the event that a contract is not successfully and expeditiously executed by the respondent initially selected for contract award.
7. Reject any or all proposals received in response to this RFP.

G. Terms and Conditions for Proposals

1. Definitions -- Please note the following definitions of terms used:
 - a) "Respondent" means the person, firm, or corporation which submits a formal quotation.
 - b) "Contractor" means the person, firm or corporation chosen to perform the duties described in this RFP

- c) "Customer" means CSI.
 - d) "MSAG" means the master street address guide.
 - e) "ALI" means Automatic Location Identification
 - f) "System Provider" means any entity that provides the entire NG9-1-1 system and is the single point of contact on an ongoing basis.
 - g) "GIS" means geographic information system.
 - h) "PSAP" means Public Safety Answering Point
- 2. Acceptance of Conditions**
Submission of a proposal indicates full acceptance by the Respondent of the conditions contained in the RFP and its attachments, unless clearly and specifically noted in the submittal.
- 3. Disclosure of Proposal Contents**
- a) CSI decisions on withholding information from public disclosure are subject to potential review by Board Counsel, the Attorney General, and the courts. CSI assumes no liability for the disclosure of any information that it is advised to disclose by Board Counsel, the Attorney General, or the courts.
 - b) The fiscal information included in the Cost Proposal will be held in confidence to the extent allowed by law and will not be disclosed to or discussed with competitors.
 - c) Technical proposals will be subject to public examination, except for clearly labeled proprietary information.
 - d) Proposals may be reviewed by persons who are not members of CSI as part of evaluation process. Any such individuals will be informed of policies related to proprietary information.
- 4. Prime Contractor Responsibility**
Respondents have the option of subcontracting parts of the services they propose. If any part of the work is to be subcontracted, the Respondent shall describe in the quotation the subcontracting organization and the contractual arrangements made therewith. All subcontractors will be subject to approval by CSI. The selected Respondent will also furnish the corporate or company name and the names of officers or principals of said companies or organizations proposed as subcontractors. CSI will consider the prime Contractor to be solely responsible in all contractual matters, including payment of any and all charges resulting from such subcontractor arrangements.

5. The winning Respondent shall cause appropriate provisions of its quotation to be inserted in all ensuing subcontracts to insure fulfillment of all contractual provisions by subcontractors.
6. **Incurred Costs**
CSI is not liable for any costs incurred by respondent in preparing their proposals, or any costs of contractors' participation in any pre-contract award activity.
7. **Taxes Not Applicable** - CSI as a governmental unit, is exempt from any and all taxes. A tax-exempt certificate will be supplied to the successful Respondent upon request.
8. **Equal Opportunity** - The Contractor will not discriminate against any employee or applicant for employment because of race, color, sex, religion, national origin, or age. The Contractor will take affirmative action to ensure that applicants are employed and the employees are treated during employment without regard to their race, color, sex, religion, national origin or age. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; requirement of advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by an appropriate agency of the federal government setting forth the requirements of these nondiscrimination provisions.
9. **Notification of Award**
After evaluation and selection of the successful Respondent(s), all Respondents will be notified in writing of CSI's decision. The names of the selected Respondent(s) will be made available to the public.
10. **Complete Services/Products** : The winning Respondent shall be required to:
 - (a) furnish all tools, equipment, supplies, supervision, transportation, and other accessories, and services.
 - (b) furnish all materials, supplies, and equipment specified
 - (c) provide and perform all necessary labor; and

- (d) execute and complete all specified work with due diligence, in accordance with good technical practice and the requirements, stipulations, provisions, and conditions of this RFP and the resultant contract.

H . Evaluation of Proposals

CSI will establish two committees. The finance committee will evaluate and compare costs of each proposal to make sure that we are comparing “apples to apples” and that all of the associated costs and options are included. The technical review committee will evaluate and score all proposals based on whether or not they meet or exceed the requirements of the RFP. They will also consider a vendor’s experience and capacity to do the project. Proposals with a total cost in excess of \$2.2 million will be set aside and only considered if those lower cost proposals fail to meet the RFP requirements. CSI may, at its sole option, elect to require presentation(s) by respondents clearly in consideration for award. CSI reserves the right to accept a proposal, or to reject any and all proposals based on what is judged to be in CSI’s best interests. CSI will endeavor to negotiate a contract with the preferred respondent. If a mutually agreeable contract cannot be negotiated with the selected respondent, CSI will then enter into contract negotiations with the next highest rated firm, and so on, until a mutually agreeable contract can be negotiated.

Evaluation Criteria

a) Application features

Contractors are asked to explain how the system performs each of the features listed in the Technical Questions and Issues.

b) Experience, Capacity and Support

The respondent should demonstrate expert knowledge in 9-1-1 system integration, IP-based call handling, GIS mapping, ALI/MSAG/GIS synchronization, data transfer and trouble-shooting. The proposals should indicate the respondent’s relevant experience in projects of similar nature, complexity and schedule. Contractors should demonstrate an ability to work with a wide range of organizations necessary for the coordination of this project.

The respondent should demonstrate an understanding of the technical issues involved with integrating a map display application into the

PSAP including interfacing with all Telco, call-taking, GIS, AVL, and CAD requirements. The technical approach should follow recognized NENA standards. Respondents should demonstrate the technical capacity to meet the specifications and schedule requested in the RFP.

I. Proposal Format and Content

To speed and simplify evaluation and to assure that each proposal receives the same orderly review, all proposals must follow the format described in this section. Proposals shall contain all elements of information requested, without exception. Proposal sections and pages shall be appropriately numbered for easy reference. To make your responses as efficient as possible you may provide information in one section and -- in later sections -- make a specific reference to the earlier material, rather than re-stating it. Proposals shall include and be organized into the following sections (detailed below):

1. Letter of Submittal with signature
2. Introduction and Executive Summary
3. Response to Technical Questions & Issues
4. Relevant Experience of Respondent
5. Customer References
6. Cost Proposal

1. Letter of Submittal:

Must be signed by duly authorized officer - Provide the following information for your firm. If you are proposing to subcontract some of the proposed work to another firm, similar information must be provided for each subcontractor.

Firm name and business address, including telephone and fax numbers.

Year established (include former firm names and year established, if applicable).

Type of ownership and parent company, if any.

2. Introduction and Executive Summary:

In the executive summary, highlight the major facts or features of the proposal including any conclusions, assumptions, and recommendations

you desire to make. The executive summary should be designed specifically for review by executives who may not possess a technical background. It should be brief and not include canned marketing materials.

- 3. Technical Features and Capabilities:** In responding, cite the question before each answer. Full, direct, and substantive answers are required. Non-specific answers will be considered unresponsive.
- 4. Customer References:** Provide a minimum of three references for projects of similar size and scope. References should include: Customer Name, Primary Contact Name, Phone Number, Email Address, Description of the solution provided; Date solution was installed; Size of installation (number of PSAPs, positions)
- 5. Relevant Experience of Respondent:** Detail previous experience implementing projects of a similar size and scope.
- 6. Cost Proposal:** This should contain an itemized (Excel format preferred) of the required and optional costs as outlined in the RFP. We love discounts; however, we don't want to see them in the spreadsheet. If you are taking off 20% on all software, state that in your cost proposal cover page, but do not show before and after figures for each line item. Do not total everything, then take off a one-time discount. The line item break down must equal the total cost. If you are going to give us a \$100,000 price break, that is great. Please reduce the costs, for example, of software, training, project management, installation etc. so that the reductions total that amount. We will determine whether or not to purchase some of the hardware ourselves by comparing your quote with what we can get off of state bids. Please indicate which items can be purchased by CSI using your specifications. We DO NOT need a break down of the cost to each individual PSAP. If we need one at each PSAP show that as a unit price times 28 PSAPs. If we need one at each position show that as a unit price times 60 positions. If identical items after the first at the same location are less expensive, show 28 times the initial cost then x times the lower price. Please break down the costs in the following manner.

- A) Hardware to be located at the two data centers. (This would include all servers, racks, UPS, network components, telephone equipment, cabling, monitors, etc.)
- B) Software that will run on the servers at the two data centers. (This would include call-handling, database management, operating system, mapping, network related, anti-virus, information management software etc.)
- C) Hardware to be located at the 28 PSAPs. (This would include work stations, telephones, routers, gateways, etc. We will provide our own monitors, racks and UPS)
- D) Software that will run on the work stations at the PSAPs. (This would include call-handling, mapping etc. Some PSAPs may choose to keep their existing GIS applications.)
- E) Professional Services for work at the data centers including project management, shipping, staging, installation, IT and administrative training, as-built documentation etc.
- F) Professional Services for work at the psaps including those listed in E plus dispatcher training
- G) Support and Maintenance – years 2-5 for software and hardware provided by the vendor. Please separate the software and hardware portions.

III. Technical Features and Capabilities

This Section defines the functional, technical, performance and professional service requirements. Where requirements indicate “Optional,” CSI may or may not select those items for purchase in the immediate procurement.

Where the term Enhanced 9-1-1 (E9-1-1) is used, it is intended to include wireless 9-1-1 Phase I and Phase II capabilities consistent with FCC Order 94-102. The use of the term “carrier” includes both wire line, wireless and alternate providers of telecommunications services.

**Each of the following enumerated items
require an affirmative or narrative response from vendors.**

Vendors are to insert their responses immediately following each requirement. Any clarification or exceptions to the requirements must be clearly stated in this narrative response. Note that changes or edits to the requirements do not supersede or replace the original text.

Proposal Compliance Codes

Vendors must provide responses to each of the Technical and Feature Requirements by using the codes outlined below. Full, direct, and substantive answers are required.

“C” Meaning

Comply – The proposed solution will fully meet this requirement because it currently exists as a standard feature or function in the base application software.

“D” Meaning

Does not comply – The proposed solution does not fully comply with this requirement. The vendor will not meet this requirement in its entirety. Please give a detailed explanation.

“T” Meaning

Available through a third party – This requirement can be met by a software module that the vendor has arranged to use through a third party contract. The unit of software or software module must be designed for seamless integration with the base application software. Vendor’s existing product Costs for the separate unit of software or module are included and clearly identified in cost quotation.

“CS” Meaning

Customize – The requirement can be met by altering the proposed software to meet the requirements and specifications. Costs for customizing software are included and clearly identified in cost quotation. Vendor also must commit to completion of any custom software as part of the initial installation.

“EX” Meaning

Explanation – Response requires an answer to a question rather than a stated requirement. Example, “What language is the application written in?” Vendor should use the “EX” code and provide answers as needed on a separate page.

NETWORK AND CARRIER CONFIGURATION	
1. Ability to support multiple types of inbound and outbound analog or digital Central Office or End Office provisioning, such as SS7, PRI/ISDN, CAMA, Feature Groups C & D, etc.	
2. Ability to provide a local termination/demarcation point for carriers while maintaining overall call routing configuration.	
3. The solution proposed must be capable of receiving both 9-1-1 and administrative call in a native SIP format upon installation.	
4. The system shall provide selective routing of inbound 9-1-1 calls based on customer-provided Emergency Service Zones (ESZ)	
5. Ability to accept automated update of Selective Routing information from MSAG processing.	
6. In the event that a primary PSAP is out of service, or that all circuits to that PSAP are out of service, 9-1-1 calls shall be routed to an alternate PSAP.	
7. The system shall provide the ability to test inbound call routing of all carriers on an on-going basis after implementation.	
8. The system shall support additional one-button transfers to other entities.	
9. Transferred calls shall provide original caller’s ANI/ESRK rather than the PSAP’s ID.	
10. Emergency callers to receive automated announcement or other indication of call status if their call is queued or not answered.	
11. Installed system to provide the capability for real-time measurement of Quality of Service for network infrastructure.	
12. Vendor to identify the specific internetworking standards and protocols to be deployed.	

NETWORK AND CARRIER CONFIGURATION

13. Vendor to identify all bandwidth requirements including between PSAPs and support facilities.	
14. Vendor to describe the configuration and protocol features that provide for reliable call handling in the case of hardware or application problems, including a call in progress scenario.	
15. System shall provide a native IP environment for the receipt of Voice over Internet Protocol (VoIP) 9-1-1 calls with associated data..	
16. Vendor to describe their integration options with administrative telephone systems for consolidation of call taking platforms.	
17. Vendor to describe expansion capabilities. System must be capable of expansion to multiple additional counties/PSAPs by simply adding additional software and hardware. Systems requiring the replacement of components to expand will not be considered.	

PSAP EQUIPMENT

1. System shall conform in all material respects to current NENA recommendations for PSAP equipment, including: a. NENA 04-001, Standards for PSAP Equipment b. NENA 04-004, Standards for PSAP Intelligent Workstations c. NENA 08-002, Functional and interface Standards NG9-1-1 (i3) d. NENA 08-501, Network Interface to IP capable PSAP e. NENA 08-502, E9-1-1 Requirements. Please explain how your solution aligns with these standards.	
2. The solution should allow the option to purchase our own hardware per specs supplied by vendor.	
3. Vendor to provide back-up SIP phone at each call taker position. SIP phone must display ANI/ALI. Vendor to describe additional capabilities of the proposed telephone instruments.	
4. Backup telephone instruments shall be provided with handsets and function independently or in parallel with the Intelligent Work Stations.	
5. Ability to place calls on hold for retrieval by any call taker (Call Park).	

PSAP EQUIPMENT

6. System shall provide Automatic Number Identification (ANI) and Automatic Location Identification (ALI) data display in a consistent format regardless of the originating carrier or routing of the call.	
7. PSAP equipment shall retrieve ALI equivalent information from customer's database system.	
8. PSAP equipment shall provide for ALI retrieval from Caller ID (Business Lines) or manually entered telephone number.	
9. System shall accommodate the handling and display of Wireless 9-1-1 Phase I and Phase II information, including Confidence and Uncertainty.	
10. Ability to support access to multiple ALI databases (e.g., to query ALI of transferred wireless 9-1-1 calls from other jurisdictions).	
11. Intelligent Workstation to provide history of prior calls at time of call presentation to call taker.	
12. Intelligent Workstation platform to support the installation of third-party applications.	
13. To the extent that peripheral network components (such as telephone instruments) outside of centralized equipment rooms require supplemental electrical power, this shall be provided via Power Over Ethernet (POE) provisioning.	
14. Ability to monitor the audio of call taking at another position, with or without muting.	
15. Ability to 'barge-in' to a call in progress by supervisory personnel.	
16. Ability to conference calls with unlimited outside parties vendor to describe any limitations.	
17. Ability to support separate inbound call queues if circuit provisioning is deployed.	
18. Ability to support one-button re-dialing of recent calls, including abandoned calls.	
19. Vendor to describe approach to capturing abandoned call information for call taker use.	
20. Ability to display location information at each call taker position for calls pending.	
21. Ability to provide system-wide status at each PSAP, reflecting system availability, calls in progress, call taker availability, and calls in queue.	
22. Allows Creation of Incoming Call Queues	
23. Allows Creation of Spatial Incoming Call Queues	
24. Ability to integrate two-way audio from telephone calls and radio traffic into one headset.	

PSAP EQUIPMENT**FUTURE PATH PLANS**

1. Vendor to describe their intended migration path to Next Generation NENA i3 architectures. Describe how your solution aligns with the current NENA, ESIF, ATIS, IETF standards today.	
2. Vendor to describe their migration path to receive Automatic Crash Notification and Telematics information with 9-1-1 calls.	

TDD/TTY

1. Ability to support Baudot-format TDD/TTY dialogue from callers at every position.	
2. Ability to provide TDD/TTY detection and alerting at each call taker position.	
3. Ability to capture and provide permanent record of TDD/TTY dialogue; vendor to describe approach to TDD/TTY call logging.	
Ability to support Instant Messaging (IM) and Short Messaging Service (SMS) and text messaging dialogue from public 'callers.'	

COMPUTER AIDED DISPATCH AND MAPPING INTEGRATION

1. System shall transfer all of the available ANI/ALI data into a CAD incident entry application, including location lat-long data.	
2. System shall provide interface to third-party or vendor mapping application for real-time display of inbound call information. Integrated mapped ALI display is preferred.	
3. Ability to support integrated mapping application co-resident on Intelligent Workstation.	

WARRANTY

1. Vendor to describe warranty services included in the proposal.	
---	--

LOGGING AND INSTANT RECALL RECORDERS

- | | |
|--|--|
| 1. Vendor to provide data logging system with capabilities to handle multi-media recording in the future. | |
| 2. Vendor to provide Instant Recall Recording and playback application software at each workstation position with the ability to integrate with existing analog voice logging recorder at each PSAP. | |

MANAGEMENT INFORMATION SYSTEMS

- | | |
|---|--|
| 1. System to provide for a Management Information System (MIS) reporting of transaction volumes and system performance for overall system as well as significant components. | |
| a. MIS and reporting application to allow access all captured database elements. | |
| b. Detail of MIS reporting to provide for both individual PSAP and system-wide transaction volumes and call handling performance. | |
| c. MIS reporting to provide for time and day of week summary reporting in tabular and graphical formats. | |
| d. Reporting application to provide for selection of indexing and sorting keys by any formatted field. | |
| e. MIS to capture and report System Availability, including alarms, error reports, and platform status. | |
| f. MIS to capture response time to PSAP ALI database inquiries and re-bids. | |
| g. MIS shall be capable of capturing data from all circuits within the system, including inbound 9-1-1 trunks, administrative lines and dedicated ring down circuits, as well as outbound calling. | |
| 2. Each data center shall be equipped with a management information system which tracks incoming calls and provides flexible real-time information and periodic reporting. Access to information shall be acquired remotely by permissions. Available information for a requested time period shall include at a minimum:
a. Number of total calls received
b. Number of abandoned calls
c. Number of calls on a per trunk/per circuit basis
d. Number of calls on a call type (wire line, wireless, VOIP, etc.) basis
e. Number of calls conference/transferred
f. Calls conference/transferred by destination (e.g., secondary PSAPs)
g. Number of calls on a log-on or per position basis
h. Average time to answer
i. Average length of call and average hold time | |

<p>3. Each data center shall be equipped with a Call Detail Record (CDR) function that provides for capture, search and retrieval, display, and printing of information regarding each 9-1-1 call:</p> <ul style="list-style-type: none"> a. Date received b. Trunk seize/call appearance time c. Caller's telephone number d. ANI, ESRK or other routing identification e. Answer time f. Answering position identification g. Trunk/circuit identification h. Time call was released i. Time call was transferred j. Transfer destination k. Abandoned call indicator l. Ringing start time m. Time call was placed on hold and taken off hold and by what position n. All ALI data, including name, address, community, ESN, Class of Service, etc. <p>Data may be accessed remotely from the psaps with permissions.</p>	
<p>4. Ability to direct MIS reports or Workstation printouts to any Local Area Network-attached printer.</p>	
<p>5. Ability to export formatted detailed records or summary report tables for analysis with third-party applications (e.g., Microsoft Office).</p>	
<p>6. MIS reporting to be fully initialized prior to operational use of system; this includes any procedures, routines and scripts for daily, monthly and annual periodic reporting.</p>	

SYSTEM ADMINISTRATION	
<p>1. Ability for the customer to administer appropriate system features and configuration without voiding warranty or support agreements.</p>	
<p>2. Ability for customer to administer call queuing and call routing parameters.</p>	
<p>3. Ability to support centralized and customer administered backup and recovery policies.</p>	
<p>4. Ability to support on-line centralized backup</p>	
<p>5. System to support use of generally available third-party platform protection products, such as anti-virus, spyware and Trojan protection applications. Vendor to specify responsibility for updates to applications and signature files.</p>	

SYSTEM ADMINISTRATION

6. Vendor to describe the implementation of end-to-end security and authentication in the proposed configuration.	
7. Ability to automatically provide outbound pager and email notification to support personnel of system events and alarms.	
8. The system shall provide real-time call volume and call status information at remote locations, including: <ul style="list-style-type: none">a. Positions Logged On/Ready/Availableb. Positions Busy/Off Hookc. Positions Not Ready/Out of Queued. Calls in Queue/Calls Pendinge. Calls Holding/Calls Parkedf. PSAP Status (e.g., system OK, connectivity good)	
9. Ability to provide a real-time display of system availability, call taker availability & calls in progress.	

SYSTEM PERFORMANCE

1. System to provide overall 99.999% availability, measured on a 24 hour per day, 7-day per week basis, accumulated over a one-year period. Vendor to clarify compliance and/or describe any exceptions.	
2. System to support automated, unassisted restoration from stoppages or outages, including significant network components and application software.	
3. System to provide positive/affirmative alert to each call taker position of off-line status, error conditions or conditional events.	
4. The system shall support localized supervision and reporting of ANI and ALI failures, network outages, etc.	
5. The system shall provide in each PSAP readily visible and (selectable) audible indicators of emergency and non-emergency calls pending.	
6. Vendor to describe their recommended approach to node and link redundancy to meet Availability Performance Requirements.	

SYSTEM PERFORMANCE

7. Vendor to describe their system architecture as it relates to failover and fault tolerance. The scope of this discussion should include the PSTN entry, the gateway into the 9-1-1 IP network, traffic paths to the network endpoints, and any crucial devices within the scope of the relevant network fabric.

MAINTENANCE AND SUPPORT

1. Vendor to provide a fixed cost for annual tier 2/ tier 3 maintenance after the warranty period. Maintenance begins at the end of the Warranty period and is defined as the resolution of application software and configuration issues at no additional cost to the customer. Vendor to provide a proposed Maintenance and Support scope of services statement with proposal response. State your warranty period
2. Vendor to provide full and complete set of technical and maintenance documentation at each primary installation location.
3. Vendor to maintain on-going trouble report tracking system and historical records of trouble reports and problem resolution.
4. Vendor to recommend a complement of essential and recommended spare parts and component assemblies to be locally maintained; on-site secure storage will be made available at each PSAP. In no case shall any component in operational use be moved or utilized as a spare.
5. Vendor to utilize remote access for system and application diagnostics and maintenance. Vendor to coordinate Virtual Private Network (VPN) or other secure access requirements with the CSI Information Technology staff.
6. As necessary to resolve Critical Issues, the vendor must anticipate the need for on-site, factory-trained staff, capable of diagnosing and supporting the installation of this platform.
7. Vendor to coordinate all maintenance activities with each PSAP. Vendor and PSAP to agree on migration checklist and notification schedule for any activities impacting operations.

CONTRACT DOCUMENTS AND PROJECT DELIVERABLES

This section identifies the Contract Documentation and Project Deliverables to be provided by the Vendor. Contract Documents will be provided before the initiation of work by the successful vendor. Project Deliverables are to be provided by Vendor at key implementation milestones.

CONTRACT DOCUMENTS AND PROJECT DELIVERABLES	
<p>1. Vendor-provided Contract Documentation to include:</p> <ul style="list-style-type: none"> a. All Software Licenses, Terms and Conditions, including third-party hardware and software. b. All Warranty Terms and Conditions specific to hardware, software and services. c. All Manufacturer or Vendor Maintenance and Support Terms and Conditions. d. Minimum specifications for customer and third-party provided equipment or facilities. 	
<p>2. Vendor-provided Project Deliverables to include:</p> <ul style="list-style-type: none"> a. Project Management Plan, provided at the initiation of the vendor’s work program. Project Management Plan to include identification of named individuals, their roles/responsibilities and contact information. Any required transmittal documents or approvals not identified in the Contract shall be identified and described in the Project Management Plan. b. Attach an Estimated Project Plan in Gantt Chart format with your proposal. c. Implementation Plan and Project Schedule to be negotiated with CSI. Plan to include description of CSI, vendor and third party responsibilities, including facility preparation requirements; any required data conversion and system migration plans; and Project Schedule to identify critical path elements and target milestone dates. <ul style="list-style-type: none"> • Training Plan, Syllabus, Training Materials and Training Schedule; documentation to be provided in advance of training sessions. Training Plan to identify any pre-requisites, duration of sessions and objectives. Syllabus to provide agenda and topics to be covered during each training session. Training Materials includes any attendee hand-outs, reference sheets, tests, presentations or other instructor-utilized materials. The Training Schedule is the calendar of training sessions, identifying planned dates and times of training sessions to be provided by the Vendor. Sufficient printed copies of End User Instruction Manuals for all attendees. d. Periodic Project Status Reports; written reports provided no less than monthly through the duration of installation project. 	

INSTALLATION, TESTING AND TRAINING

1. Physical installation work by vendor shall utilize best industry practices and adopted national standards.	
2. All cables and demarcation points are to be clearly labeled. All cables are to be bundled and secured to avoid disconnection during normal use and servicing access.	
3. All cables installed in workstation furniture shall be provided in a length to accommodate the full range of workstation motion, as well as providing for access and removal for servicing.	
4. All interface components (e.g., impedance or protocol matching boxes) shall be labeled and secured.	
5. Vendor to coordinate all on-site activities to minimize disturbances to dispatch operations at each PSAP. Vendor to provide prompt and timely notice of any potentially public safety service-impacting activity.	
6. Proposed training schedules to be coordinated and mutually agreed to with no less than two weeks notice.	
7. Vendor shall provide training to an initial cadre of system users and administrators. Vendors will anticipate providing some training sessions outside normal hours to accommodate call taker schedules.	
8. The solution should allow for CSI's IT personnel to be trained to provide primary on-site Tier 1 support of the system.	
9. Vendor to include a brief description of the training courses that will be offered and which customer personnel should attend.	
10. Vendor to describe Customer responsibilities for training.	

SYSTEM MONITORING

1. Proposed system to provide error logs and diagnostic information sufficient to support vendor troubleshooting. Vendor and/or Customer to provide any additional hardware components or application software required to diagnose reported Critical or Serious issues.	
--	--

MASTER CLOCK SUBSYSTEM

- | | |
|--|--|
| 1. Vendor to ensure that the master clock subsystem shall provide NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) time synchronization outputs for additional information systems, such as: <ul style="list-style-type: none">a. Computer Aided Dispatchb. Database and Communications Serversc. Logging Recorders | |
| 2. The master clock subsystem shall provide a time synchronization source to all PSAPs. | |

INTEGRATED IP-BASED PBX (OPTIONAL)

1. Must be software based.
2. Must enable seamless transfers between the 9-1-1 system and IP-PBX.
3. Must have built-in failover to allow admin calls to be processed by 9-1-1 system if IP-PBX is unavailable.
4. Must include extensions (phone and mailbox) that can have multiple phones connect to it from the same extension number.
5. Minimum features must include: Auto Attendant ; Conference ; Hunt Group; Agent Group; Calling Card (DISA); Paging; Service Flag; and IVR Node
6. Must include as an option call recording to enable the recording of all calls on an extension at all times. Recording should take place for inbound calls from hunt group, agent group, all internal calls, all external calls or both internal and external calls.
7. Proposer must specify all associated costs including maintenance and support of the IP-PBX solution in the Price Proposal. These costs should be listed as a separate option for purchase.

OPTIONAL – GIS DATABASE MANAGEMENT SYSTEM
To follow are the requirements for a GIS data management solution.

Type & Section	Technical and Feature Requirement Question	Response Code	
General Features	1.1	Can edit the following GIS layers: Roads, Sites, Driveways, Landmarks, ESZ, ESA, Hydrology, Utility Lines, Railroads, Town boundaries	
	1.2	Application must automatically read wireless data from a standard wireless carrier file and build <i>or</i> update the tower point file and the sector coverage areas.	
	1.3	Provide for the import of the Telco MSAG and provide automatic matching with the GIS road data	
	1.4	Allow for the automated updates from other users of the software. The updates must be selectable by region or date. (E.g. import only the records after a particular date or in a particular region)	
	1.5	Allow export of a “Public Data Set” that excludes personal information	
	1.6	Provides for the export of CAD Data and CAD “Geofiles”	
	1.7	Provides for the creation and export of a wireless ALI Database that may be used for spatially routing phase 2 wireless calls	
	1.8	Application must provide a set of evacuation tools	
	1.9	Create any number of evacuation zones (radius, custom, etc.)	
	1.10	Produce a dialing list for all TNs in any/all evacuation zones directly from the ALI database or a pre-processed ALI database	
	1.11	Application must allow export of data by date, region or manual selection	
	1.12	Application must import/export Telco MSAG	
	1.13	Application must import/export ALI database	
	1.14	Application must link ALI records to sites	
	1.15	Application must link MSAG records to named road segments	
	1.16	Display the GPS point and line trace data of each driver in the field symbolized by driver and day in the field. GPS trace should also be symbolized to show differentially corrected points clearly from non-corrected points.	
	1.17	Build ESZ directly from Telco MSAG	
	1.18	Provide 1-click polygon merge/explode	
	1.19	Provide a selection control that allows one-by-one review of any selected set. The control must zoom to the location of each feature as it is selected for review.	
	1.20	Zoom In/Out, Zoom to Lat/Long, Zoom to any site, road, ESN, ESA, etc.	
	1.21	Conflate attribute information between any two sets of road data or any two sets of polygon layers	
	1.22	Provide for an enhanced, quick method to capture sites and/or driveways from digital orthos or other imagery	
	1.23	Application must provide a quality control system that assures proper assignment of road names to site addressing	
	1.24	Application should provide a control for Pan & Zoom in a controlled manner for organized review of data	

Type & Section		Technical and Feature Requirement Question	Response Code
	1.25	Image data (digital orthophotos) can be selected automatically without manual interpretation of image location	
	1.26	Road naming, address labeling, town labeling, etc. is performed automatically with non-overlapping labels of all features from the attribute information of each layer.	
	1.27	Manual labeling must be an option.	
	1.28	Find any address, site or named road quickly	
	1.29	Application must provide a simple backup and restore function	
	1.30	Application provides an auto-geocoding function that will update the road centerline address ranges based on the actual site addresses adjacent to each road segment <i>or</i> minimum and maximum address range on each segment based on the addressing increment used on the road or the average increment along the road. The min/max function must not allow overlapping ranges between segments.	
	1.31	Application can display tax map data and any other layers	
	1.32	Show map units in Degrees-Minutes-Seconds or Projected Units	
	1.33	Automatically import new and verified data from the field including site pictures	
	1.34	Import/Export functions to move data to/from field for verification and collection.	
	1.35	Automatically receive and setup up for the review of GIS discrepancies captured by call-takers	
	1.36	Developed on ESRI ArcGIS 9.3	
	1.37	Interfaces with ESRI ArcSDE (Enterprise, Workgroup, Personal, File)	
	1.38	Manages data in personal geodatabase and enterprise Geodatabase	
	1.39	Interfaces with Microsoft SQL Server 2005 and/or 2008	
1.40	Integrates with microDATA's map display software (ALI-Trakker or xTrakker) and data field collection software (x9Collector)		
Site Maintenance (address point data)	2.1	Edit site location & attributes: address, zip, resident, units, access, site type, picture, grand-father status, side-of-road, etc.	
	2.2	Addressing maintains new <i>and</i> old addresses	
	2.3	Auto-addressing of new/existing sites according to standard	
	2.4	Auto-addressing of an entire road or township with one mouse click	
	2.5	Synchronization with GIS addresses with ALI addresses	
	2.6	Maintains Emergency Service Zone for each site	
	2.7	Maintains Township for each site	
	2.8	Automatic notification for illogical or mis-numbered sites	
	2.9	Maintain pictures and/or floor plans	
	2.10	Maintains resident unit information for each site an each unit within the building or site	
	2.11	Maintains verification status of GPS field work at site	

Type & Section		Technical and Feature Requirement Question	Response Code
2.12-2.23	2.12	Provides addressing based on access point, building or driveway location	
	2.13	1-click for address at any point, or picture of any site	
	2.14	Adjust addresses on a single road by a given amount	
	2.15	Reverse the addressing on a road	
	2.16	Prepare completely automated notification letters	
	2.17	User-definable text for any number of letters	
	2.18	Auto merge from entered data	
	2.19	Each letter includes a map of addressed location	
	2.20	Each letter includes a picture of the building at that location	
	2.21	Maintains USPS Class file for easy update by USPS	
	2.22	Maintain links to USPS, Assessor, and Utilities	
	2.23	Unit data with name and matched TN and utility meter number	
3.1-3.11	3.1	Road naming and Segment Address Ranges	
	3.2	Road names managed from a single table	
	3.3	Maintain official name, 3 Aliases, and the ALI Name	
	3.4	Provide any standard addressing method, increment, rules	
	3.5	Synchronization with MSAG road names	
	3.6	Connectivity Audits to assure that road segments connect	
	3.7	Add, Edit, Move, Snap, Split while maintaining geocoding	
	3.8	Can view by road direction or road class	
	3.9	Maintain Route #, Class, Address Range, Direction	
	3.10	Provide an auto-extend function to avoid manual splitting of intersecting roads when adding a new road	
	3.11	Automatic field verification update	
4.1-4.8	4.1	Reshape/Drag ESZ boundaries to change selective transfer	
	4.2	Auto-update of MSAG from ESZ	
	4.3	Add a new ESZ with/without new ESN definition	
	4.4	Maintain ESN definitions	
	4.5	Maintain Emergency Service Agency (ESA) information	
	4.6	View ESZ by PSAP, Law, Fire, EMS	
	4.7	ESZ/Wireless sector viewing/analysis – Allow overlay of wireless sector coverage areas over ESZ jurisdictions to view or determine the likely ESZ. ESN determination must be available in a completely automated mode or with manual override.	
	4.8	ESZ, ESN, ESA, MSAG, completely integrated with sites and roads	

Type & Section		Technical and Feature Requirement Question	Response Code
Development tools	5.1	Automated structure checker for all databases used in the application. If the structure is incorrect, the application must automatically correct the structure. If the layer/file does not exist it must make a new empty file ready for input.	
	5.2	Has a concatenation function to join information from two or more fields into one field	
	5.3	Auditing – Application must provide the following audits:	
	5.4	Complete log of all changes including date and user	
	5.5	Unique road naming, duplicate ARC-ID check	
	5.6	Problem address report – Correct parity, In proper order, Duplicate addressing, Proper road name, etc.	
	5.7	Site address assessment report	
	5.8	Sites with no address <i>or</i> roads with no address ranges	
	5.9	Find Coincident sites	
	5.10	Site addresses have correct road name, ESN, side-of-road, etc.	
	5.11	Road segment connectivity	
	5.12	Geocoding address range check	
	5.13	Road, site, ESZ, landmark, etc. data have valid attributes	
	5.14	ESZ has valid ESN; ESN has valid ESA; etc.	
Map Generation & Maintenance	6.1	Create atlas map books	
	6.2	Detailed road and site map books (atlases) production	
	6.3	Atlas sheet development, maintenance	
	6.4	Map book covers and street index production	
	6.5	ESN map books	
	6.6	Large scale regional map sheets (up to 36"x48")	
	6.7	Maintains standard address, average increment address and grand-fathered (previous) address. Choose any for ALI.	
Wireless Data Preparation	7.1	Automatic development of wireless layers	
	7.2	Automatic entry of wireless tower/sector data from standard	
	7.3	Entry of cell-site by form or map entry	
	7.4	Editing of cell-sector areas	
	7.5	Visibility analysis based on terrain	
	7.6	Assign PANI's or cell-sector ID's and notify carriers of such assignment	
	7.7	Maintenance of ALI wireless database	
	7.8	Display of all or filtered set of towers	
	7.9	Automatic determination of expected ESN	
	7.10	Select sector for editing from table or map	
	7.11	Select any set of sectors for simultaneous display	
	7.12	Handle CAS or NCAS ID assignment	
Collection and Mapping	8.1	Provides an integrated GPS collection and verification program that provides the following features:	
	8.2	Standardized field display of 9-1-1 layers integrated with GPS	

Type & Section		Technical and Feature Requirement Question	Response Code	
	8.3	Display moves with GPS and shows current location and trace		
	8.4	Display allows editing in real-time of captured data		
	8.5	Automatic import/export of sites requiring verification		
	8.6	View, auto-link with ALI, USPS, Utility and Assessor databases		
	8.7	Sites are “thrown” based on laser range-finder bearing & distance		
	8.8	Automatic linkage and storage of digital pictures		
	8.9	Quality control check of side-of-road and road name		
	8.10	Collection of sites, landmarks, roads and driveways.		
	8.11	Verification of address, location, road name, type of use, picture, side-of-road, addressing point, etc.		
	8.12	Stores location specific comments to be reviewed by GIS tech.		
	8.13	Provide comments from GIS tech for field review		
	8.14	All data entry, moves, adds, etc. logged for supervisor review		
	8.15	One-button click for end-of-day file transfer to office GIS		
	8.16	Form driven to capture all pertinent 9-1-1 information		
	ALI-Synchronization	9.1	Import ALI, MSAG, Daily Service Orders (DSO), MSAG Change Orders	
		9.2	Uses GIS data maintained above as source for data to synchronize with ALI data	
9.3		Synchronize MSAG-Road names; ALI-Site address; ALI-Road segments; MSAG-road range; DSO-Site address; DSO-Road segment; MCO-road seg.		
9.4		Maintains a local copy of ALI database from changes		
9.5		Maintains TN-site link for evacuation		
9.6		Audit reports of fall-out		
9.7		Handles all NENA and Bell standard formats		

Proposer must specify all associated costs including maintenance and support a of the GIS database management solution in the Price Proposal. These costs should be listed as a separate option for purchase.

<p style="text-align: center;">LOCALLY MAINTAINED AUTOMATIC LOCATION DATABASE Requirements for a locally managed “XXXXX” automatic location database.</p>

ALI Database Management

1. Need to conform to current NENA standards and recommendations for database management (or better alternate), including:
 - NENA 02-010: Recommended Formats & Protocols For ALI Data Exchange, ALI Response & GIS Mapping.
 - NENA 02-011: Recommended Data Standards for Local Exchange Carriers, ALI Service Providers & 9-1-1 Jurisdictions.
 - NENA 06-001: Recommended Standards for Local Service Provider Interconnection Information Sharing.
2. Need to provide systems and procedures for promptly updating subscriber information in ALI databases; “Customer” goal is one business day turn-around between entities (e.g., from carrier to aggregator)
3. Need to update ALI databases with carrier service order completion records within one business day; “Customer” goal is overnight processing of error-free records.
4. Need to provide database record integrity with multiple sources of information and multiple carriers when using Local Number Portability (LNP).
5. Need to support comprehensive carrier ALI record transaction sets (e.g., record migrate, lock/unlock, etc.)
6. Need prompt system responses to ALI data inquiries (i.e., from initial ringing, call answer or repoll).
7. Need to support electronic submission of database error reports to carriers from dispatch centers (e.g., web-enabled form, electronic mail or alternate).
8. Need to provide Master Street Address Guide (MSAG) for carriers to validate Service Order addresses and installation locations.
9. Need for Master Street Address Guide (MSAG) to capture and maintain Emergency Service Numbers (ESN) for address ranges.
10. Ability to receive and integrate Private Switch ALI (PS-ALI) information from carriers or third parties such as PBX owners.
11. Ability to electronically utilize “Customer” ESRI GIS data for record validation (i.e., use GIS data as master validation source).

12. Need to provide for electronic export of ALI and MSAG information in format compatible for cross-validation with GIS information.

Future Path Plans

1. Vendor to describe the migration path to NENA Version 4, XML architecture. (NENA 02-010)
2. Vendor to describe plans for migration to NENA Next Generation i3 VoIP and telematics ALI architecture and the use of an Emergency Services Query Key (ESQK).

Wireless 9-1-1

1. The proposed system shall capture and display the full call back number (CBN) of domestic calling parties.
2. The proposed system shall display the Emergency Services Routing Key (ESRK) of the incoming call.
3. The proposed system shall display the Wireless Carrier Name Identification; NENA or FCC Carrier ID as option,
4. ALI display shall display wireless carrier Class of Service codes (i.e., wireless phase designation).
5. The proposed system shall capture and display tower identifier and antenna sector identification on ALI displays and through CAD interface data streams.
6. The proposed system shall provide the street address and related information (latitude/longitude) of tower and sector.
7. The wireless 9-1-1 ALI database shall accept dynamic updates from a wireless Mobile Position Center (MPC). The Contractor shall refer to J NENA recommendations for the Implementation of the Wireless Emergency Service Protocol E2 Interface via TCP/IP.
8. ALI display information shall include Confidence and Uncertainty factors if provided by the wireless carrier.
9. ALI architecture to support multiple re-bids from dispatch centers; provide dynamic Phase II location updates if supported by carrier.

Administrative Requirements

1. Capability to generate canned and custom system reports. It is expected that such reports would include but would not be limited to:

1. TN Tally Report
2. TN Tally Report by Community
3. Service Order Fallout Report
4. Service Order Update Report
5. Service Order Updates 24 Hour Report
6. Service Order Processing Statistics Report
7. Service Order Corrections Statistics Report
8. Service Order Processing Errors Report
9. Service Order Error Codes Report
10. MSAG Updates Report
11. NRF Summary and Detail Reports
12. MSAG Overlaps Audit Report
13. MSAG Parity Report
14. MSAG Change Requests Report
15. ALI Audit: GIS site match Report
16. TNs by Community for Liaisons Report
17. Unnumbered Addresses Report

Proposer must specify all associated costs including maintenance and support a of the ALI database management solution in the Cost Proposal. These costs should be listed as a separate option for purchase.

INTEGRATED MAPPED-ALI DISPLAY

TECHNICAL FEATURES AND CAPABILITIES

1.1 Minimum Requirements

There are a number of minimum requirements that must be met by the proposed solution in order to provide a Mapped-ALI solution. These minimum requirements for the proposed solution includes

- 1.1.1 The map display must utilize ESRI based standards for the mapping object libraries. The map must be built on ESRI ArcGIS 9.3 or newer platform.
- 1.1.2 Interfaces with NENA standard 9-1-1 Call Processing Equipment
- 1.1.2 Wireless Phase 1 and Phase 2 compliant.
- 1.1.3 Capture map errors and/or discrepancies.
- 1.1.4 Complete integration with vendor's GIS Data Management System.
- 1.1.5 Ability to display CAD and AVL events on the map.

1.2 Functional Requirements

Certain functional requirements, which are necessary to perform the tasks necessary for Mapped-ALI are listed below. For each requirement, proposer should include a detailed description of the proposed functionality and process.

- 1.2.1 The application must have the ability to interface with and display digital orthophotos as well as have the ability to display other raster image data libraries.
- 1.2.2 The primary data source for the mapping application will be ESRI based data.
- 1.2.3 A legend must be available to the call-taker allowing any layer to be turned "on" or "off".
- 1.2.4 The Lat/Long of the current position of the mouse cursor must be able to be displayed.
 - 1.2.4.1 Lat/Long must be available in decimal degrees (DD), degrees - minutes -seconds (DMS), degrees-decimal minutes (DDM), State Plane and UTM.
- 1.2.5 Map symbology must be based on attributes within the GIS data.

1.2.6 Application must include a separate window displaying the entire map area or an area significantly larger than is displayed in the map window.

1.2.7 Application must be able to search for a caller provided address or location to facilitate the determination of the emergency providers and facilities at that address or location.

1.2.8 The mapping application must automatically display the tower and sector coverage area and the information provided by the CAS or NCAS solution for Phase I wireless calls.

1.2.9 The mapping solution must automatically display the lat/long and information provided by the CAS or NCAS solution for Phase II wireless calls. Symbol must change based on the latest class of service of the call

1.2.10 Application must include an automated means of capturing ALI discrepancies and spatial discrepancies and reporting those back to a designated location.

1.2.11 Application must provide a call history to easily return to a prior call for remapping or entry of discrepancy information.

1.2.12 Mapping system must have an easy method of updating each component of the map display system including: Configuration changes – System administrator must be able to make configuration changes in a central location and “push” the configuration to desired workstations.

1.2.13 GIS data updates – GIS data will be maintained on site and in centralized locations. The mapping system must provide the functionality to provide automated updates of the GIS data at each call taking station over a WN/LAN.

1.2.14 Print/Fax: Application should be able to print a map on a local or network printer or Fax a map to a secondary provider.

1.2.15 Must include ability to display oblique imagery such as Pictometry’s software.

1.2.16 Proposer must specify associated costs and the details of maintenance and support of the Mapped ALI solution in the Pricing Proposal. These costs should be listed as a separate option for purchase.

General Features

Ability to automatically display wireline, wireless Phase I and II, VoIP calls and ALI rebids.

Ability to view all active and prior call events in the system or PSAP, and all agent calls answered during the current session.

Ability to bookmark an unlimited number of preset map views.

Ability to customize user interface based on user permissions.

Ability to use layer caching for faster map loading.

Ability to create multiple and distinct map displays.

Ability to choose from shape and symbology options to create drawings on the map display (local or enterprise).

Ability to view ToolTips for site locations; ToolTips can include address information, geocoder match score and site picture(s).

Application must be NG9-1-1 ready.

Application must be built on the most current ESRI ArcGIS Engine (9.3.1).

Ability to support several geodatabase options, including Personal SDE, Workgroup SDE, Enterprise SDE, and File Geodatabase.

Allows for real-time GIS data updates.

Ability to answer a call directly from the map.

Allows for one-click dialout to response agencies directly from the map.

Ability to dispatch from the map.

Searching Options

Ability to conduct multiple searches simultaneously.

Ability to return and zoom to search results for an exact address search.

Ability to return and zoom to geocoded search results for an approximate match of a searched address.

Ability to display "geocoder match scores" that rank search results for approximate matches of address searches.

Ability to return and zoom to search results for an intersection.

Ability to return and zoom to configurable "common place" locations.

Ability to search for an exit or mile marker.

Ability to perform a coordinates search using either Lat/Lon or x,y coordinates.

Ability to search for ESNs and associated response agencies.

Discrepancy Management

Ability to create map discrepancies from active or previous calls, or create from scratch (ad-hoc).

Ability to display map discrepancies for agent only, PSAP only and entire system.

Ability to create ALI discrepancies from active or previous calls, or from scratch.

Ability to display ALI discrepancies for agent only, PSAP only and entire system.

Map Navigation

Ability to "grab" and move the map display around without changing the viewing scale (pan).
Ability to measure distance and area using a variety of measure units (measure tool).
Ability to zoom in and zoom out using either a preset or user-determined scale.
Ability to quickly zoom to a predefined scale or manually enter a zoom scale .
Ability to select a layer or multiple layers and view the "raw" GIS data in the database (identify tool).
Ability to search the GIS data for information without needing pre-configured locators (find tool),
Ability to scroll around the map in all directions (roam).
Application must include a generalized, smaller-scale map (such as an overview map) that shows the limits of another map's extent along with its surrounding area.
Ability to display an electronic legend of map layer symbology (Table of Contents).

Imagery
Ability to access image catalogs to display aerial imagery, orthographical photos and other scanned images.

AVL, CAD and ENS Integration
Ability to automatically display AVL and CAD events on one map or on several maps.
Ability to provide emergency notification systems (ENS) operations directly from the map display.