Next Generation 9-1-1 Security (NG-SEC) Audit Checklist

NENA Next Generation 9-1-1 (NG-SEC) Audit Checklist
NENA 75-502, Version 1, December 14, 2011
Development Steering Council Approval Date, November 1, 2011
Standards Advisory Committee Approval Date, November 22, 2011
NENA Executive Board Approval Date, December 14, 2011

Prepared by:
National Emergency Number Association (NENA) Joint Technical and Operations Security for Next Generation 9-1-1 Working Group.

Published by NENA

Printed in USA

NENA

INFORMATION DOCUMENT

NOTICE

The National Emergency Number Association (NENA) publishes this document as an information source for the designers and manufacturers of systems to be utilized for the purpose of processing emergency calls. It is not intended to provide complete design specifications or parameters or to assure the quality of performance for systems that process emergency calls.

NENA reserves the right to revise this Information Document 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 interface or services described herein.

It is possible that certain advances in technology will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) 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 System Service 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's Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Acknowledgments:

The National Emergency Number Association (NENA) Operations and Technical Committee Chairs developed this document. NENA recognizes the following industry experts and their companies for their contributions in development of this document.

Version 1, Approval Date, 12/14/2011

Members	**Company/Agency**
Smith - CISSP, Jeremy - Working Group Technical Co-Leader	L.R. Kimball
Vanauken, Gordon - Working Group Operations Co-Leader	L.R. Kimball
Vislocky, Mike – CPE Chair	Network Orange, Inc.
Walthall - CISSP, Robert CPE Vice Chair	National Public Safety Solutions
Boyken, Bill	AT&T
Davis, Kenneth	Sangamon County ETSD
Erdman, Bob	Amcom Software
Herron, Myron S	Synergem
Irwin, Dave	Washington Military Department, Emergency Management Division
Kaczmarczyk, Casimer M	Verizon
Kelley, Robert	
Lagreid, Steve	King County E9-1-1 Program
Lewis, Shelby	Positron
Lipinski, Jim	State of VT
Mathis, CISSP ENP PSNP, Ron	Intrado Inc.
McClure, ENP, Nate	AECOM
McIntire, Clay	North Central Texas Council of Governments
Oenning, Bob	State of Washington
Rodabaugh, Carl	
Rosen, Brian	NeuStar

Schoenberg, Carter	Motorola
Skain, John	Clinton County 9-1-1
Sylvester, Robert L.	Convergent Technologies, Inc.
Wilcox, Nathan G	microDATA

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. The committee/working group would also like to give a special thank you to Kenneth Davis for support & assistance in formatting the original standard into the checklist format.

TABLE OF CONTENTS

1 Executive Overview

This Information Document is a companion to the **NENA 75-001 - NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) Standard**. To effectively use this document the user should have a clear understanding of the concepts and procedures described therein.

This checklist provides a summary of the requirements and recommendations detailed in the NG-SEC standard and provide the educated user a method to document a NG-SEC Audit. The checklist has spaces to document the findings of the audit.

The auditor can use this document to record if the 9-1-1 entity complies or not with the listed item. There is also room to make notes of the findings. Each checklist item is further categorized as:

- R – Requirement
- BP – Best Practice

The date and auditor's identity should also be documented, including cases where multiple auditors may be used.

2 Introduction

2.1 Operations 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 Technical Impacts Summary

Certain security features of various 9-1-1 equipment may be impacted 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.

2.3 Security Impacts Summary

This security checklist references the NG-SEC standard which may impact other NENA standards. Accordingly it should be reviewed by each NENA committee to determine impact.

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
NENA 75-502	12/14/2011	Initial Document
NENA 75-502.1	05/25/2015	Update web page links

2.6 Recommendation for Additional Development Work

No additional standards work was identified, but continued updates to the NG-SEC documents will be needed to keep them current.

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

This checklist is available for use immediately, and may take several days to complete the checklist.

2.9 Costs Factors

The implementation of this checklist will have costs of the time to complete the checklist. Additional cost to implement the recommendations of the NG-SEC Standard as identified by the use of this checklist.

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

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

2.12 Additional Impacts (non-cost related)

The information or requirements contained in this NENA document are expected to have 9-1-1 technical and center operational impacts, based on the analysis of the authoring group. At the date of publication of this document, development had not started. The primary impacts are expected to include:

- Time needed to complete this checklist
- Changes to operational procedures
- New equipment
- New staff skill sets

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
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

2.14 Acronyms/Abbreviations

Acronyms/abbreviations used in this document have been included in the original standard document 75-001.

3 Operations or Technical Description

The following instructions and clarifications are provided to guide the auditor.

- For each section, provide the auditor name, title, and contact information, as well as the date the audit section was completed
- For each audit question, choose C for "comply," No for "does not comply" or not applicable (N/A) for "the requirement is not applicable." If N/A is chosen, provide commentary as to why the question isn't application in the comments column. Items marked No are deemed out of compliance with the NG-SEC standard.
- Please refer to the NG-SEC standard (NENA Document 75-001) itself as a reference for questions of interpretation.
- As noted earlier, audit questions consist of Requirements (R) and Best Practices (BP).
- For questions or sections not audited please indicate they were not audited using the comments column

Section 1 - Senior Management Statement

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
1	4.1	Has Senior Management created a Senior Management Statement (SMS) of Policy? (Audit Guidance: this could take the shape of a security plan, executive level security policy, or other such documents. The auditor should use his/her discretion as to whether the document in question meets the requirements of this portion of the NG-SEC standard)	R	☐ C ☐ No ☐ N/A	
2	4.1	Does the SMS designate the person responsible for security (e.g. Security Administrator)?	R	☐ C ☐ No ☐ N/A	
3	4.1	Does the SMS clearly document the security goals and objectives of the organization?	R	☐ C ☐ No ☐ N/A	

Section 1 - Senior Management Statement Auditor:_____ Date:_____

Section 2 - Acceptable Use Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
4	4.2	Does the organization have an Acceptable Usage Policy?	R	☐ C ☐ No ☐ N/A	
5	6.6	Are any and all actual, attempted, and/or suspected misuses of Public Safety assets reported and documented by appropriate organizations?	R	☐ C ☐ No ☐ N/A	

Section 2 - Acceptable Use Policy Auditor:_____ Date:_____

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
6	4.2	Does the organization have an Authentication / Password Policy?	R	☐ C ☐ No ☐ N/A	
7	7.1.1	Is each individual requiring access to the NG9-1-1 System provided a unique Identification and authentication?	R	☐ C ☐ No ☐ N/A	
8	7.1.1	Do individuals share their authentication information (including usernames and passwords) with other individuals or groups?	R	☐ C ☐ No ☐ N/A	
9	7.1.2	Are requests for new User Accounts, User IDs, and File and Resource authorization documented? (Audit Guidance: review applicable documentation and processes for adequacy of process and adherence to process)	R	☐ C ☐ No ☐ N/A	
10	7.1.2	Do personnel performing entity or security administration ensure that only approved entities are granted access?	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
11	7.1.2.1	Does the organization have procedures for changing access authority?	R	☐ C ☐ No ☐ N/A	
12	7.1.2.1	Does the organization have procedures for removing access authority for terminated personnel?	R	☐ C ☐ No ☐ N/A	
13	7.1.3	When system to system access is implemented does the system mask individual accountability for transactions? (Audit Guidance: The system shall not mask individual accountability for transactions)	R	☐ C ☐ No ☐ N/A	
14	7.1.3	When system to system access is implemented is the source system authenticated before each transfer session?	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
15	7.1.3	When system to system access is implemented and push technology is utilized, is the destination authenticated by the source?	R	☐ C ☐ No ☐ N/A	
16	7.1.3	When system to system access is implemented and a continuous connection is utilized, was authentication performed at the initial connection?	R	☐ C ☐ No ☐ N/A	
17	7.1.3	When system to system access is implemented are individuals accessing any of the systems required to Authenticate when initially accessing each system?	R	☐ C ☐ No ☐ N/A	
18	7.1.5	Are Authentication Credentials displayed in an obscured format when entered on computer screens? (Auditor Guidance: Check to see if passwords can be seen on the screen when typed in. They should not be able to be seen so as to prevent "shoulder surfing.")	R	☐ C ☐ No ☐ N/A	
19	7.1.4	Are users locked out after no more than 5 invalid sign on attempts?	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
20	7.1.5	Are Default and Null Passwords changed when installing new equipment or software?	R	☐ C ☐ No ☐ N/A	
21	7.1.5	Are Authentication Credentials encrypted when stored on a computer?	R	☐ C ☐ No ☐ N/A	
22	7.1.5	When two-factor authentication is used, (e.g. SecurID + Pin or Certificate + Passphrase) are two authentication factors stored in such fashion that one incident can compromise both? (Auditor Guidance: e.g. password or pin isn't written down on the token, or stored with the token)	R	☐ C ☐ No ☐ N/A	
23	7.1.5.1	All user accounts shall require a password	R	☐ C ☐ No ☐ N/A	
24	7.1.5.1	Passwords are not based on the user's account name.	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
25	7.1.5.1	Passwords must meet the following complexity requirements: • Contains characters from three of the following four categories: ○ Uppercase alphabet characters (A–Z) ○ Lowercase alphabet characters (a–z) ○ Arabic numerals (0–9) ○ Non-alphanumeric characters (for example, !$#,%)	R	☐ C ☐ No ☐ N/A	
26	7.1.5.1	Minimum password length shall be 8 characters or greater	R	☐ C ☐ No ☐ N/A	
27	7.1.5.1	Minimum password age shall be 3 days or greater	R	☐ C ☐ No ☐ N/A	
28	7.1.5.1	Maximum password age **requirement** 60 days or less	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
29	7.1.5.1	Maximum password age **recommendation** 30 days	BP	☐ C ☐ No ☐ N/A	
30	7.1.5.1	If 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.	R	☐ C ☐ No ☐ N/A	
31	7.1.5.1	When using temporary passwords they shall be required to be changed upon initial login	R	☐ C ☐ No ☐ N/A	
32	7.1.5.1	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.	BP	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
33	7.1.5.1	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	BP	☐ C ☐ No ☐ N/A	
34	7.1.5.1	Passwords should not contain sequences of three (3) or more characters from the user's login ID or the system name.	BP	☐ C ☐ No ☐ N/A	
35	7.1.5.1.4	Passwords should not contain sequences of three (3) or more characters from previous chosen or given passwords.	BP	☐ C ☐ No ☐ N/A	
36	7.1.5.1.5	Passwords should not contain a sequence of two (2) or more characters more than once, e.g., a12x12.	BP	☐ C ☐ No ☐ N/A	
37	7.1.5.1.5	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.	BP	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
38	7.1.5.2	When Passphrases are used do they have a required length of at least 15 characters? (Audit Guidance: Alpha, numeric and special characters may all be used.)	R	☐ C ☐ No ☐ N/A	
39	7.1.5.2	When Passphrases are used they shall not use repeating words, or sequential characters or numbers.	R	☐ C ☐ No ☐ N/A	
40	7.1.5.2	When Passphrases are used they shall be case sensitive		☐ C ☐ No ☐ N/A	
41	7.1.5.2	When Passphrases are used and where they are automatically set or set by administrator, the initial passphrase shall be randomly generated and securely distributed.	R	☐ C ☐ No ☐ N/A	
42	7.1.5.2	When Passphrases are used first-time users may create their own passphrase after authenticating.	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
43	7.1.5.2	When Passphrases are used Users shall have the capability of changing their own passphrase online. However, the old passphrase shall be correctly entered before a change is allowed	R	☐ C ☐ No ☐ N/A	
44	7.1.5.2	When Passphrases are used a lost or forgotten passphrase can be reset only after verifying the identity of the user (or process owner) requesting a reset.	R	☐ C ☐ No ☐ N/A	
45	7.1.5.2	When Passphrases are used passphrases shall automatically expire every 180 days or less for General Users.	R	☐ C ☐ No ☐ N/A	
46	7.1.5.2	When Passphrases are used systems shall notify users at expiration time and allow the user to update the passphrase.	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
47	7.1.5.2	When Passphrases are used and when it 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.	R	☐ C ☐ No ☐ N/A	
48	7.1.5.2	When Passphrases are used systems shall not display the passphrase in clear text as the user enters it.	R	☐ C ☐ No ☐ N/A	
49	7.1.5.2	When Passphrases are used shall not be stored in script files or function keys.	R	☐ C ☐ No ☐ N/A	
50	7.1.5.2	When Passphrases are used Passphrases shall always be encrypted for transmission	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
51	7.1.5.3	If Digital Certificates are used is a revocation procedure in place if compromised?	R	☐ C ☐ No ☐ N/A	
52	7.1.5.3	Are Digital Certificates kept current and expired or invalid certificates not used?	R	☐ C ☐ No ☐ N/A	
53	7.1.5.3	Cryptographic implementations use standard implementations of security applications, protocols, and format?	R	☐ C ☐ No ☐ N/A	
54	7.1.5.3	Cryptographic implementations shall be purchased from reputable vendors?	R	☐ C ☐ No ☐ N/A	
55	7.1.5.3	If Cryptographic solutions are developed in-house staff should be properly trained in cryptology.	R	☐ C ☐ No ☐ N/A	
56	7.1.5.3	Do employees protect and safeguard any encryption keys for which they are responsible?	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
57	7.1.5.3	Employees do not share private encryption keys with others except when applicable or appropriate authorities demand the key be surrendered (Termination, Promotion, Investigation etc.)	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
58	7.1.5.3	A process exists by which current validity of a certificate can be checked and a certificate can be revoked Validity testing includes: • Do key holders initiate key revocation when they believe access to their keys have been compromised • Has the Certificate Authority signature on the certificate been validated • Is the date the certificate is being used within the validity period for the certificate • The Certificate Revocation List for the certificates of that type are checked to ensure they have not been revoked • 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)	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
59	7.2.6	In order to help assure segregation of duties, developers shall not be System Administrators for the Production Systems they have developed (small, stand-alone systems can be excepted from this requirement)	R	☐ C ☐ No ☐ N/A	

Section 3 - Authentication / Password Policy Auditor:_____ Date:_____

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
60	4.2	Does the organization have a Data Protection Policy?	R	☐ C ☐ No ☐ N/A	
61	6.2	Application, system, and network administrators perform a security self-review on systems for which they have operational responsibility at least once per year.	R	☐ C ☐ No ☐ N/A	
62	6.2	The self-review assessments are in writing and retained by the Security Manager and the NG9-1-1 Entity	R	☐ C ☐ No ☐ N/A	
63	6.2	A copy of the current security self-review or security assessments/audit reports are retained until superseded by another security assessment or the system is retired	R	☐ C ☐ No ☐ N/A	
64	6.3	Application, system, and network administrators have identified which security solutions have or require periodic review and the frequency by which they shall occur (Auditor Guidance: This finding refers to recurring security solutions, such as audit logs, or Intrusion Prevention Systems.)	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
65	6.3	Application, system, and network administrators conduct the periodic reviews defined in audit number 64	R	☐ C ☐ No ☐ N/A	
66	6.4.2	All networks have a clearly defined purpose or mission so appropriate security measures can be implemented. (Auditor Guidance: To verify if this has occurred request documentation such as drawings, mission statements, policies, etc., that clearly indicate that the network in question's mission is defined)	BP	☐ C ☐ No ☐ N/A	
67	6.4.3	For systems on the network in question, an accurate and current inventory is maintained. (Auditor Guidance: Request copies of a current inventory. Acceptable inventories included automated systems, paper logs, or logbooks).	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
68	6.4.3	Inventories are appropriately classified and in accordance with the implemented information classification and protection policy	R	☐ C ☐ No ☐ N/A	
69	6.4.4	All administrative access to the network is precisely controlled with appropriate identification, authentication, and logging capabilities	R	☐ C ☐ No ☐ N/A	
70	6.4.4	Uncontrolled points of entry are not allowed on the network	R	☐ C ☐ No ☐ N/A	
71	6.4.4	All point of ingress and egress to a network are fully documented, approved, and protected	R	☐ C ☐ No ☐ N/A	
72	6.4.5	Connecting multi-homed computers to networks that have different security postures is not allowed	R	☐ C ☐ No ☐ N/A	
73	6.4.5	When multi-homed computers are implemented Host IPS shall be installed on the multi-homed computer	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
74	6.4.5	When multi-homed computers are implemented, all other appropriate security countermeasures, including those described in this document are implemented on multi-homed computer	R	☐ C ☐ No ☐ N/A	
75	6.4.5	When multi-homed computers are implemented Anti-virus is running on both/all networks and the multi-homed computer	R	☐ C ☐ No ☐ N/A	
76	6.4.5	When multi-homed computers are implemented, IP-forwarding is explicitly disabled?	R	☐ C ☐ No ☐ N/A	
77	6.4.5	When multi-homed computers are implemented multi-homed computers should have 'Hardened Operating Systems'	BP	☐ C ☐ No ☐ N/A	
78	6.4.5	When multi-homed computers are implemented multi-homed computers should have 'Hardened Applications'	BP	☐ C ☐ No ☐ N/A	
79	6.4.6.3	Firewalls are maintained at all 4.9GHz network boundaries	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
80	7.1.2.2	Does the organization have procedures for reviewing access authority for inactive accounts?	R	☐ C ☐ No ☐ N/A	
81	7.2.1	Accounts shall be created based on "Least Privilege"	R	☐ C ☐ No ☐ N/A	
82	7.2.1	Are users given access to only the functions and data necessary to perform their assigned duties	R	☐ C ☐ No ☐ N/A	
83	7.2.1	All computer resource access is restricted to only the command, data, and systems necessary to perform authorized functions	R	☐ C ☐ No ☐ N/A	
84	7.2.1.1	All data has appropriate minimum access privileges, e.g. read, write, modify, as defined by the data owner and is in compliance with local laws	R	☐ C ☐ No ☐ N/A	
85	7.2.1.2	Access is restricted to only those individuals and groups with a business need, and subject to the data's classification.	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
86	7.2.1.2	Unrestricted/global access should be avoided whenever possible and is only used where specifically appropriate and with the data owners approval	BP	☐ C ☐ No ☐ N/A	
87	7.2.1.2.a	Is 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.	R	☐ C ☐ No ☐ N/A	
88	7.2.1.2.b	Is group membership restricted only to persons performing the given function?	R	☐ C ☐ No ☐ N/A	
89	7.2.1.3	All unnecessary services and network services are disabled.	R	☐ C ☐ No ☐ N/A	
90	7.2.1.3	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 is disabled	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
91	7.2.1.3a	Is an annual review for compliance with Audit Area 90 completed and findings documented?	R	☐ C ☐ No ☐ N/A	
92	7.2.1.3a	Are findings from the audit conducted in Audit Area 92 closed or has the risk been managed?	R	☐ C ☐ No ☐ N/A	
93	7.2.1.4	Administrator shall ensure that system access controls (e.g. filters that restrict access from only authorized source systems), are used where they exist and only contain necessary system authorizations?	R	☐ C ☐ No ☐ N/A	
94	7.2.1.4.a	Is an annual review for compliance with Audit Area 93 completed and findings documented?	R	☐ C ☐ No ☐ N/A	
95	7.2.1.4.a	Are findings from the audit conducted in Audit Area 94 closed or has the risk been managed?	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
96	7.2.1.5	Do Administrators use non-Administrative accounts when performing non-Administrative tasks? (Auditor Guidance: The Administrator should maintain two user accounts. One with Administrator / privileged rights and one without. When performing administrative functions they should use their Administrator account. When not performing such tasks they use a "normal" user-level account. The use of "runas" or "superuser" features is allowable).	R	☐ C ☐ No ☐ N/A	
97	7.2.1.6	Do ALL System Administrators have a personal Administrator account rather than use a generic account? (Auditor Guidance: Administrators shall not use default, or built-in Administrator accounts except during disaster recovery or initial installations. Each Administrator must have his or her own unique Administrator account to provide traceability. Administrator accounts shall never be shared)	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
98	7.2.1.6	Systems that do not support unique administrative accounts should not be used as they pose a significant threat. Entities are encouraged to prevent inclusion of such systems onto the NG9-1-1 networks. .	BP	☐ C ☐ No ☐ N/A	
99	7.2.2	The login "Warning Notice" is displayed during the boot up or logon sequence (either before or after the authentication, preferably before, but it is displayed before any substantive data	R	☐ C ☐ No ☐ N/A	
100	7.2.2	The "Warning Notice" remains displayed until positive action by the user is taken to acknowledge the message	R	☐ C ☐ No ☐ N/A	
101	7.2.3	Computer resources, systems, applications, and networks shall be restricted at all times to authorized personnel	R	☐ C ☐ No ☐ N/A	
102	7.2.3	Where possible access control is accomplished with "role bases" privileges that assign users to roles and grant access to members of a role rather than to individuals	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
103	7.2.4	Non-privileged users do 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.	R	☐ C ☐ No ☐ N/A	
104	7.2.4	Only administrative users are assigned passwords to access and modify sensitive files/resources	R	☐ C ☐ No ☐ N/A	
105	7.2.5	Files/File Folders are restricted to only those requiring access	R	☐ C ☐ No ☐ N/A	
106	7.2.5	Rights assigned only to those who actually need them and are documented as needing them	R	☐ C ☐ No ☐ N/A	
107	7.2.5	Access Groups used whenever possible to simplify administration	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
108	7.2.5	Has the organization renamed built-in Administrator accounts?	R	☐ C ☐ No ☐ N/A	
109	7.2.5	Anonymous and/or guest accounts are disabled to prevent exploitation	R	☐ C ☐ No ☐ N/A	
110	7.2.5	Are periodic audits of user account access conducted to ensure users have only the "effective rights" required to perform their functions?	R	☐ C ☐ No ☐ N/A	
111	7.2.6	Are Production and Non-Production systems separated to protect integrity of the Production System?	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
112	7.2.6	If the Non-Production System is intended to become a Production System is it governed by the requirements of a Production System (Auditor Guidance: While it is unlikely a non-production system will be "in-scope" during an audit, if it is, this requirement refers to the need for that system to comply with all requirements herein)	R	☐ C ☐ No ☐ N/A	
113	7.2.6	Production data is not copied off the system without the service owner's permission and is protected to an equivalent or greater degree	R	☐ C ☐ No ☐ N/A	
114	7.2.6	Production systems do not contain any software development tools except where essential for the application	R	☐ C ☐ No ☐ N/A	
115	7.2.6	While software development tools may be installed for software upgrades, or installation of new software packages, or for troubleshooting, but they must be removed immediately after use	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
116	7.2.6	When software development tools are essential for production operation, they must be inaccessible to users	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
117	7.2.7	All devices capable of enforcing a password protected screensaver or a keyboard lock do so with an inactivity timeout of 15 minutes or less exceptions will comply with Para 7.2.7.1, .2,and .3 The following are exceptions: • When superseded by local public safety policy • 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 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 • 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	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
118	7.2.7	All devices not capable of enforcing a password protected screensaver or a keyboard lock will have controlled access in accordance with all applicable physical and logistical security or have session inactivity timeouts set for 15 minutes	R	☐ C ☐ No ☐ N/A	
119	7.2.7	Consoles not capable of enforcing a password protected screensaver or a keyboard lock are configured to automatically log out after 15 minutes of inactivity	R	☐ C ☐ No ☐ N/A	
120	7.2.7	If automatic inactivity logout is not supported are users required to logout when console is left unattended	R	☐ C ☐ No ☐ N/A	
121	7.2.8.4	Peer to Peer Networking is NOT allowed in the NG 9-1-1 environment	R	☐ C ☐ No ☐ N/A	
122	7.3.1	NG9-1-1 Entity information which is either discoverable or otherwise requested by the general public or media must be clearly identified.	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
123	7.3.1	Specific guidelines must be written and followed to document what data is released, when and to whom when releasing NG9-1-1 Entity information which is either discoverable or otherwise requested by the general public or media must be clearly identified.	R	☐ C ☐ No ☐ N/A	
124	7.3.1	The guidelines identified in Audit Area 123 shall capture any specific release requirements for data such as video, names, call content, message text, or other personal content	R	☐ C ☐ No ☐ N/A	
125	7.3.1	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	BP	☐ C ☐ No ☐ N/A	
126	7.3.2	Where email is used to send NG 9-1-1 Sensitive Information, is the message clearly marked with its classification, do the senders ensure recipients are aware of the safeguards required.	R	☐ C ☐ No ☐ N/A	
127	7.3.2	Where email is used for emergency communications, senders must verify the recipient's email ID is correct prior to sending	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
128	7.3.2	Where email is used for emergency communications, the recipient shall understand the safeguards associated with the proprietary marking	R	☐ C ☐ No ☐ N/A	
129	7.3.2	Where email is used for emergency communications and email with Sensitive Information is printed it shall be protected according to the rules associated with its classification	R	☐ C ☐ No ☐ N/A	
130	7.3.2	Where email is used for emergency communications, Sensitive Information must be encrypted when sent by email	R	☐ C ☐ No ☐ N/A	
131	7.3.2	Does the NG9-1-1 entity control the domain used for email communication unless otherwise covered by a formal contractual document (Auditor Guidance: The intent of this audit question is to ensure that entities register a legitimate DNS domain name for any NG9-1-1 communication as opposed to using free email services, etc.).	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
132	7.3.2	Internal NG9-1-1 Entity email should not be made available on a 9-1-1 call-taking position workstation, but rather on a separate system.	BP	☐ C ☐ No ☐ N/A	
133	7.3.2	In lieu of detailed security standards for email use in an NG9-1-1 environment, NG9-1-1 Entities are encouraged to follow best practices such as those offered by the National Institute for Standards and Technology (NIST)	BP	☐ C ☐ No ☐ N/A	
134	7.3.2.1	Individual messaging services have been evaluated to ensure they comply with NG9-1-1 Entity production and security requirements	R	☐ C ☐ No ☐ N/A	
135	7.3.3.1	Do cryptographic installations use industry standard cryptographic algorithms and standard modes of operations and comply with the laws of the United States	R	☐ C ☐ No ☐ N/A	
136	7.3.3.1	The use of encryption algorithm or device complies with the laws of the United States and any country in which there are plans to use data encryption	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
137	7.3.3.1	It is recommended the algorithm certified by the NIST FIPS 140 certification, currently AES, be used	BP	☐ C ☐ No ☐ N/A	
138	7.3.3.1	Where there are no US federal standards for specific encryption functions e.g. public key cryptography, message digests, commercial algorithms may be used.	BP	☐ C ☐ No ☐ N/A	
139	7.3.3.1	Implementations of cryptography shall follow best commercial practices e.g. Public Key Cryptography Standards.	R	☐ C ☐ No ☐ N/A	
140	7.3.3.1	Implementations and modes shall use the strongest available product	R	☐ C ☐ No ☐ N/A	
141	7.3.3.2	If Public Key Cryptography is used does the NG9-1-1 entity have a Public Key Infrastructure to manage and distribute public keys?	R	☐ C ☐ No ☐ N/A	
142	7.3.3.2	Does the PKI manage both Symmetric and Asymmetric Keys through the entire life cycle?	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
143	7.3.3.2	Encryption Devices and any server used to store encryption keys are protected from unauthorized access	R	☐ C ☐ No ☐ N/A	
144	7.3.3.2	Key generation is performed using a commercial tool that comply with x.509 standards and produce x.509 compliant keys.	R	☐ C ☐ No ☐ N/A	
145	7.3.3.2	Keys are not generated using predictable function or values	R	☐ C ☐ No ☐ N/A	
146	7.3.3.2	Symmetric keys must be at least 112 bits in length and Asymmetric keys at least 1024 bits in length	R	☐ C ☐ No ☐ N/A	
147	7.3.3.2	Keys are distributed to appropriate recipients through secure channels	R	☐ C ☐ No ☐ N/A	
148	7.3.3.2	Keys used to secure stored data are safeguarded so authorized persons can recover them at any time	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
149	7.3.3.3	Does the Public Key Infrastructure (PKI) have a documented Certificate Practice Statement defining how security is provided for the infrastructure, registration process, relative strength of the system, and Legitimate uses?	R	☐ C ☐ No ☐ N/A	
150	7.3.3.3	Does the PKI implement a registration process that identifies the requester by an acceptable form of identification before the Certificate Authority (CA) creates a Digital Certificate?	R	☐ C ☐ No ☐ N/A	
151	7.3.3.3	Does the PKI have a review process for validity checks and revocation as required?	R	☐ C ☐ No ☐ N/A	
152	7.3.3.3	Do key holders initiate key revocation if they believe access to their keys have been compromised?	R	☐ C ☐ No ☐ N/A	
153	7.4.1	Are all files and software scanned for viruses and malicious code, and verified as free of logic bombs or other malicious code?	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
154	7.4.3	Does the NG 9-1-1 entity use licensed industry standard antivirus (or anti-malware) software on all devices capable of running it?	R	☐ C ☐ No ☐ N/A	
155	7.4.3	Does the NG 9-1-1 entity, install and maintain the latest version (including engine) of their licensed anti-virus software?	R	☐ C ☐ No ☐ N/A	
156	7.4.3	Is the antivirus software installed and maintained on any personal equipment used for business functions?	R	☐ C ☐ No ☐ N/A	
157	7.4.3	Is the software current with the latest available and applicable virus definitions?	R	☐ C ☐ No ☐ N/A	
158	7.4.3	Does the software scan all files when opened and/or executed (including files on network shares)?	R	☐ C ☐ No ☐ N/A	
159	7.4.3	Does the software scan files on local drives at least once a week?	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
160	7.4.3	Does the software scan all files, attachments, and software received via email and/or downloaded from websites before opening?	R	☐ C ☐ No ☐ N/A	
161	7.4.3	Does the software scan all removable media and software (including new workstations equipped with pre-loaded software) before opening and/or executing?	R	☐ C ☐ No ☐ N/A	
162	7.4.3	Does the NG 9-1-1 Entity scan all removable media and software before opening and/or executing if it has not been kept secure within its control?	R	☐ C ☐ No ☐ N/A	
163	7.4.3	Are all files made available as network shares scanned at least once per week?	R	☐ C ☐ No ☐ N/A	
164	7.5.4	Does the NG 9-1-1 Entity have a backup procedure?	R	☐ C ☐ No ☐ N/A	
165	7.5.4	Is a copy of the routine full backup media described in Audit Area 164 sent to a secure offsite location?	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
166	7.6	All systems, applications, and databases have internal controls for logging, tracking, and personnel accountability	R	☐ C ☐ No ☐ N/A	
167	7.6.1	All systems, including but not limited to applications and databases, have a security event record(log) capable for after-the-fact investigation of loss, impropriety, or other inappropriate activity	R	☐ C ☐ No ☐ N/A	
168	7.6.2	A written Security Audit Log Review Plan has been developed	R	☐ C ☐ No ☐ N/A	
169	7.6.3	A Security Alarm Plan has been developed and documented which sets criteria for generating alarms, who is notified, and what actions are to be taken.	R	☐ C ☐ No ☐ N/A	
170	8.3	Sensitive data is printed only on attended printers or on printers in a secured area. Distribution is controlled and printouts of sensitive information are secured when not in use.	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
171	8.3	Data stored on removable media that are external to the system hardware is safeguarded.	R	☐ C ☐ No ☐ N/A	
172	8.3	Personal storage devices are not used within the NG9-1-1 entity location. (Auditor Guidance: Examples of personal storage devices include USB Thumbstick, etc.)	R	☐ C ☐ No ☐ N/A	
173	8.3	When storage media and output is destroyed it is in a manner that contents cannot be recovered or recreated	R	☐ C ☐ No ☐ N/A	
174	8.3	When producing copies containing classified, the originals and copies are not left unattended	R	☐ C ☐ No ☐ N/A	
175	8.3	NG9-1-1 Entity personnel ensure re-used storage media is "clean" (i.e. does not contain any residual of information from previous uses)	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
176	8.3	All media distributed outside NG9-1-1 Entity is either new or comes directly from a recognized pool of "Clean" media	R	☐ C ☐ No ☐ N/A	
177	8.4.2	If possible, information resources using a power supply are connected to electrical outlets and communications connections that utilize surge protection	BP	☐ C ☐ No ☐ N/A	
178	8.6.2.10	Combustible materials are not stored in the computer center or server room	R	☐ C ☐ No ☐ N/A	
179	8.6.2.11	Furniture, storage cabinets, and carpets are of nonflammable material.	R	☐ C ☐ No ☐ N/A	
180	8.6.2.12	Carpets are anti-static.	R	☐ C ☐ No ☐ N/A	
181	8.6.2.6	All critical information resources are on UPS	R	☐ C ☐ No ☐ N/A	

Section 4 - Data Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
182	8.6.2.7&.8	Food, drinks, or smoking is not allowed in the server room	R	☐ C ☐ No ☐ N/A	
183	8.6.2.9	Storage under raised floors or suspended ceilings is prohibited.	R	☐ C ☐ No ☐ N/A	

Section 4 – Data Protection Auditor:_____ Date:_____

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
184	12	An Exception Approval / Risk Assessment process is in place.	R	☐ C ☐ No ☐ N/A	
185	12	The exception approval and risk acceptance process includes Risk Justification, Risk Identification, Risk Assessment, Risk analysis, and Risk Acceptance and Approval.	R	☐ C ☐ No ☐ N/A	
186	12	The exception approval and risk acceptance process is documented on each Exception Approval / Risk Acceptance Form (EA/RAF), including the names and contact information of the people who carried out the analysis.	R	☐ C ☐ No ☐ N/A	
187	12.1	The EA/RAF process is followed for "ALL RISKS" (e.g., security vulnerabilities cannot be fixed or security patched, or cases of non-compliance with this Security Standard.	R	☐ C ☐ No ☐ N/A	
188	12.1	The specific non-compliance or vulnerability documented in each EA/RAF was reviewed by NG9-1-1 Entity security organization and the legal department.	R	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
189	12.1	The actual form is maintained and tracked by the NG9-1-1 Entity Security Risk Manager, the Security Point of Contact, and all involved parties.	R	☐ C ☐ No ☐ N/A	
190	12.2.1	The NG9-1-1 Entity has assigned a Security Risk Manager to manage security risks and is responsible for completing the EA/RAF in a complete and accurate manner prior to submitting to the Security Point of Contact / Team for review.	R	☐ C ☐ No ☐ N/A	
191	12.2.1	The Security Risk Manager collaborates with other members of the pertinent security team in completing the form and obtains the approval signature from the NG9-1- Entity Risk Acceptance Approver.	R	☐ C ☐ No ☐ N/A	
192	12.2.1	The Security Risk Manager is an employee or an authorized agent acting on behalf of the NG9-1-1 Entity.	R	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
193	12.2.1	The Security Risk Manager is the person identifying the need for the execution of the exception approval and risk acceptance process with technical and business knowledge of the asset(s) at risk or, meets 195	R	☐ C ☐ No ☐ N/A	
194	12.2.1	The Security Risk Manager is a system administrator, systems engineer, project manager, or other key stakeholder with technical and business knowledge of the asset(s) at risk.	R	☐ C ☐ No ☐ N/A	
195	12.2.1	The Security Risk Manager acts as Point of Contact for the organization owning the identified asset(s) at risk within the scope of the exception approval and risk assessment process for the duration of the EA/RAF	R	☐ C ☐ No ☐ N/A	
196	12.2.1	If the Security Risk Manager leaves the entity or is changes job during the active duration of the EA/RAF, a new Security Risk Manager is identified to fill the role	R	☐ C ☐ No ☐ N/A	
197	12.2.2	A Security Point of Contact / Team is assigned to review for completeness, accuracy, and consistency and subject matter expertise.	R	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
198	12.2.2	For high level risks, a team of Subject Matter Experts (SME) is assembled to review, document concurrence, and sign the EA /RAF prior to submission for final approval.	R	☐ C ☐ No ☐ N/A	
199	12.2.3	Has the senior official of the NG9-1-1 Entity has signed forms accepting complete accountability for any identified risk?	R	☐ C ☐ No ☐ N/A	
200	12.3	Risks to the NG9-1-1 Entity are acknowledged, assessed, and managed according to their severity.	R	☐ C ☐ No ☐ N/A	
201	12.3	Responsibility is not delegated to subordinates or peers, and adheres to the management level or higher.	R	☐ C ☐ No ☐ N/A	
202	12.3	The Risk Acceptance Approver is the senior manager with financial and legal responsibilities for the services and operation of the specific NG9-1-1 Entity.	R	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
203	12.3.1	The NG9-1-1 entity manages the process flow as noted below: 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 3. Manager until agreement reached or no more progress possible, involve a team of SMEs as necessary. 4. NG9-1-1 Entity Security Risk Manager signs EA/RAF. 5. The Security POC / Team documents concurrence position and signs the form 6. 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. 7. 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. 8. The Security Risk Manager, Security POC / Team, and Risk Acceptance Approver as well as other involved parties	R	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
204	12.3.2	The entity tracks and documents risks in accordance with the chart provided in Appendix A.	R	☐ C ☐ No ☐ N/A	
205	12.4	Risk assessments are reviewed periodically in compliance with the following timeframes: • Critical 0 Months • High 3 Months • Medium 6 Months • Low 12 Months	R	☐ C ☐ No ☐ N/A	
206	12.5	Any change to the circumstances identified in the EA/RAF that affect the associated risk is immediately documented and submitted through the EA/RAF process.	R	☐ C ☐ No ☐ N/A	
207	12.6.1-.3	When conducting risk assessments, vulnerability assessments, and impact assessments they should be conducted using the guidance provided in sections 12.6Risks are identified and assessed IAW Para 12.6.1 through 12.6.3.	BP	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
208	12.6.8	The EA/RAF should comply with the requirements of Para 12.6.8.	BP	☐ C ☐ No ☐ N/A	

Section 5 - Exception Request / Risk Assessment Auditor:_____ Date:_____

Section 6 - Hiring Practices

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
209	4.2	Does the organization have a Hiring Practice Policy?	R	☐ C ☐ No ☐ N/A	

Section 6 - Hiring Practices Auditor:_____ Date:_____

Section 7 - Incident Response

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
210	13 & 4.2	Has a formal, written Incident Response Plan detailing how the organization will respond to a computer security incident been created?	R	☐ C ☐ No ☐ N/A	
211	7.2.6	Are software and/or data changes initiated due to outage/recovery process documented and retained until it is determined the production system and data were not corrupted?	R	☐ C ☐ No ☐ N/A	
212	7.5.5	Have Business Continuity/Disaster Recovery (BC/DR) procedures been developed and tested?	R	☐ C ☐ No ☐ N/A	
213	7.5.5	Do the plans allow for the 'Worst Case' event (i.e. Incident Recovery outside 50 miles from normal location)?	R	☐ C ☐ No ☐ N/A	
214	7.5.5	Are BC/DR drills conducted at least annually?	R	☐ C ☐ No ☐ N/A	

Section 7 - Incident Response Auditor:_____ Date:_____

Section 8 - Information Classification and Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
215	5	Does the organization have an Information Classification and Protection Policy that encompasses both administrative and production systems?	BP	☐ C ☐ No ☐ N/A	
216	5.10.1	Does the organization have disposal procedures for hard copy or printed sensitive data?	BP	☐ C ☐ No ☐ N/A	
217	5.10.2	Does the organization have sanitation procedures for media/devices containing sensitive data?	BP	☐ C ☐ No ☐ N/A	
218	5.2.1	Have Data **Owner** responsibilities been defined?	BP	☐ C ☐ No ☐ N/A	
219	5.2.2	Have Data **Custodian** responsibilities been defined?	BP	☐ C ☐ No ☐ N/A	
220	5.2.3	Are Data Classifications defined and used?	BP	☐ C ☐ No ☐ N/A	

Section 8 - Information Classification and Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
221	5.4.6	Is sensitive data received from a third party treated as if it were internal sensitive data?	BP	☐ C ☐ No ☐ N/A	
222	5.5	When receiving information where the classification of information is unknown, does the organization treat it 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?	BP	☐ C ☐ No ☐ N/A	
223	5.6	Does the organization protect classified information from unauthorized access?	BP	☐ C ☐ No ☐ N/A	
224	5.7	Does the organization encrypt stored or transmitted classified information using AES Encryption Algorithm?	BP	☐ C ☐ No ☐ N/A	
225	5.7	Does the organization have a policy for removing Mobile Computing Devices with classified data from the NG9-1-1 Entity?	BP	☐ C ☐ No ☐ N/A	

Section 8 - Information Classification and Protection

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
226	5.8	Does the entity utilize recorded/certified delivery for transporting sensitive data or media/devices containing sensitive data?	BP	☐ C ☐ No ☐ N/A	

Section 8 - Information Classification and Protection Auditor:_____ Date:_____

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
227	4.2	Does the organization have a Physical Security Policy?	R	☐ C ☐ No ☐ N/A	
228	6.5	Does the Public Safety entity require annual Security Awareness Training?	R	☐ C ☐ No ☐ N/A	
229	6.5	Have all Public Safety employees completed the annual Security Awareness Training?	R	☐ C ☐ No ☐ N/A	
230	6.6	Does the entity have procedures for reporting any suspicious or unusual activity which may indicate an attempt to breach the Public Safety networks and systems?	R	☐ C ☐ No ☐ N/A	
231	8	Is the entity is physically secured and protected from theft, misappropriation, misuse, and unauthorized access, and damage?	R	☐ C ☐ No ☐ N/A	
232	8.1	Doors with security mechanisms shall not be propped open.	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
233	8.1	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.	R	☐ C ☐ No ☐ N/A	
234	8.1	Each person entering a controlled access facility shall follow the physical access control procedures in place for that facility.	R	☐ C ☐ No ☐ N/A	
235	8.1	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.	R	☐ C ☐ No ☐ N/A	
236	8.1	When automated access control and logging devices are installed, personnel shall use them to record their entry and exit.	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
237	8.2.1	Personnel authorized with reoccurring unescorted access do not loan or share physical access devices or codes with another person?	R	☐ C ☐ No ☐ N/A	
238	8.2.1.1	Non-employees granted reoccurring access are sponsored by NG9-1-1 management personnel?	R	☐ C ☐ No ☐ N/A	
239	8.2.1.1	Does the facility's Physical Security Policy comply with all federal, state, and local laws?	R	☐ C ☐ No ☐ N/A	
240	8.2.1.2	Identification badges containing a picture of the holder shall be issued to all residents of buildings containing information resources.	R	☐ C ☐ No ☐ N/A	
241	8.2.1.2	Are ID Badges with picture issued to all residents of buildings containing information resources	R	☐ C ☐ No ☐ N/A	
242	8.2.1.2	If the facility is guarded, identification badge is displayed to the guard on entry?	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
243	8.2.1.2	Are persons on NG9-1-1 Entity premises required to present identification badges for examination and/or validation upon request?	R	☐ C ☐ No ☐ N/A	
244	8.2.1.2	Building residents and non-residents with reoccurring access who do not have a valid identification badge in their possession are signed in and vouched for by an authorized building resident who possesses and displays a valid picture identification badge?	R	☐ C ☐ No ☐ N/A	
245	8.2.1.2	Are temporary identification badge issued to all persons who do not have a permanent identification badge when entering the facility?	R	☐ C ☐ No ☐ N/A	
246	8.2.1.2	Are persons who do not have a permanent identification badge escorted while in the facility?	R	☐ C ☐ No ☐ N/A	
247	8.4.1	All portable computing devices in work areas are kept physically secure?	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
248	8.4.1	When equipped with locks, portable computing devices are kept locked to prevent theft.	R	☐ C ☐ No ☐ N/A	
249	8.4.1	Keys are stored in a secure location	R	☐ C ☐ No ☐ N/A	
250	8.4.1	Docking station style portable devices are stored in a secure location when not in use.	R	☐ C ☐ No ☐ N/A	
251	8.4.1	Docking station style portable devices are not left unattended outside normal working hours even when in the docking station	R	☐ C ☐ No ☐ N/A	
252	8.4.1	Other portable devices are stored in a locked cabinet, drawer, or office (not just the building) when not in use	R	☐ C ☐ No ☐ N/A	
253	8.4.1	Extra security precautions are implemented in and around the receiving, staging, assembly, and storage areas used for large deployments of portable computing devices	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
254	8.4.2	Vigilance is maintained in airport luggage inspection and transfer areas, hotel check in and checkout areas and other public areas	R	☐ C ☐ No ☐ N/A	
255	8.4.2	Devices are not left unattended in conference rooms, etc.	R	☐ C ☐ No ☐ N/A	
256	8.4.2	Devices are not exposed to extreme heat or cold.	R	☐ C ☐ No ☐ N/A	
257	8.5	Information resources are protected by a UPS system and/or a 'mirrored site' second location not subject to the same power outage.	R	☐ C ☐ No ☐ N/A	
258	8.5	All buildings and critical support facilities have protective physical measures in place.	R	☐ C ☐ No ☐ N/A	
259	8.6.1	Server Rooms, Data Centers, Wire Closets, and any other critical locations have limited and controlled access 24/7/365.	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
260	8.6.1	Raised floors or suspended ceilings do not allow physical access to limited access areas.	R	☐ C ☐ No ☐ N/A	
261	8.6.2.1	The facility has a fire protection/detection system which meets code and is maintained and inspected at regular intervals.	R	☐ C ☐ No ☐ N/A	
262	8.6.2.2	If sprinkler systems are provided, fire retardant polyethylene sheeting is readily available to protect media and equipment.	R	☐ C ☐ No ☐ N/A	
263	8.6.2.4	Cooling equipment is installed and in good working order.	R	☐ C ☐ No ☐ N/A	
264	8.6.2.5	HVAC systems are used to maintain environmental conditions meeting manufacturer's requirements and are supported by backup power systems dedicated.	R	☐ C ☐ No ☐ N/A	
265	8.7.1	Network equipment and access to cabling and physical wiring infrastructure are secured with appropriate physical access controls.	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
266	8.7.2	Active network jacks and connections are located only in physically secured locations (i.e., entity owned or leased space, in locked cabinets, or protected by locked physical barriers).	R	☐ C ☐ No ☐ N/A	
267	8.7.3	Unused network connections are disabled or removed in a timely manner.	R	☐ C ☐ No ☐ N/A	
268	8.7.4	Network Media are selected and located so as to minimize the possibility of wiretapping, eavesdropping, or tampering.	R	☐ C ☐ No ☐ N/A	

Section 9 - Physical Security Auditor:_____ Date:_____

Section 10 - Compliance Audits & Reviews

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
269	11	Internal audits are, at minimum, conducted annually.	R	☐ C ☐ No ☐ N/A	
270	11	Findings from such assessments are subject to corrective actions and are applied to the satisfaction of the auditing entity.	R	☐ C ☐ No ☐ N/A	
271	11	External security audits are conducted at a minimum, once every 3 years	R	☐ C ☐ No ☐ N/A	
272	11	Security audits utilize various methods to assess the security of networks and processes, applications, services, and platforms Suggested methods include automated tools, checklists, documentation review, penetration testing, and interviews	R	☐ C ☐ No ☐ N/A	

Section 10 - Compliance Audits & Reviews Auditor:_____ Date:_____

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
273	7.2.8.1	Before deployment of new forms of communication, a risk assessment should be conducted in accordance with: • The impact of resource availability • The 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 • The false positive rate (e.g. the possibility this new form of communication can generate false alarms while there are no security vulnerabilities) • The false negative rate (e.g. the potential of unknown new vulnerability is introduced by this new technology while the vulnerabilities are undetected) • The legal status (e.g. liability, contract language, recording as evidence, authority to access information, and privacy limitations) • The volume (normal, bandwidth, latency, diversity/redundancy induced denial of service etc.)	BP	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
274	4.2	Does the organization have a Remote Access Policy?	R	☐ C ☐ No ☐ N/A	
275	9	No remote access is permitted to any NG9-1-1 Entity unless addressed by contract, employee policy, or similar legal instrument which contains adequate security language as determined by a security professional?	R	☐ C ☐ No ☐ N/A	
276	9.1	Networks are segmented by business and technical functions to allow appropriate levels of protection be created while not placing unneeded restrictions on lesser risk areas	R	☐ C ☐ No ☐ N/A	
277	9.1	All boundaries and points of ingress and egress are clearly defined for each network?	R	☐ C ☐ No ☐ N/A	
278	9.1.1	Firewalls have been established at all boundary points to control traffic in and out? .	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
279	9.1.1	Firewalls use "fail all" as default?	R	☐ C ☐ No ☐ N/A	
280	9.1.1	Application Layer Firewalls are in use (recommended)	BP	☐ C ☐ No ☐ N/A	
281	9.1.10	Firewall logs are retained in accordance with applicable information retention requirements?	R	☐ C ☐ No ☐ N/A	
282	9.1.10	Logs are replicated off of the firewall?	BP	☐ C ☐ No ☐ N/A	
283	9.1.11	Identification, authentication, and access rights to log data are controlled to preserve the chain of custody for evidentiary purposes?	R	☐ C ☐ No ☐ N/A	
284	9.1.2	Access through firewalls is governed by an established policy defining clear guidelines for what is or will be allowed?	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
285	9.1.3	At a minimum, restriction of source and destination IP addresses are specific to individual addresses?	R	☐ C ☐ No ☐ N/A	
286	9.1.3	The security risks for every host or platform within the network range or subnet are evaluated?	R	☐ C ☐ No ☐ N/A	
287	9.1.4	The Firewall Administrator has minimized the number of ports exposed or permitted though the firewall? Clarifying note: the firewall administrator should be employing the least-access necessary privilege to ensure that only the necessary ports required for operation are permitted through the firewall.	R	☐ C ☐ No ☐ N/A	
288	9.1.5	All Firewall Administrators are highly qualified and experienced and 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), networking, routing, LAN/WAN technologies and	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
		associated security implications? (Auditor Guidance: Qualifications considered are, industry and or vendor certifications with various firewall products)			
289	9.1.6	Is the use of ports used by the operating system or infrastructure functions and features across network boundaries strictly controlled at the firewall?	R	☐ C ☐ No ☐ N/A	
290	9.1.7	Firewall rules are reviewed at least once per year to verify continued need?	R	☐ C ☐ No ☐ N/A	
291	9.1.8	Firewalls are accessed at least annually to address vulnerabilities identified since the last inspection?	R	☐ C ☐ No ☐ N/A	
292	9.1.9	All firewalls must log traffic with at minimum, source and destination addresses and ports are captured along with relevant time stamps and actions by the firewall.	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
293	9.2	No remote access is allowed to any NG9-1-1 Entity unless addresses by contract, employee policy, or similar legal instrument which contains adequate security language as determined by a security professional	R	☐ C ☐ No ☐ N/A	
294	9.2.1	Client based VPNs and/or consolidated modem pools are operated by NG9-1-1 Entity security personnel or personnel contracted for the purpose.	R	☐ C ☐ No ☐ N/A	
295	9.2.1	Strict control is maintained for the 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	R	☐ C ☐ No ☐ N/A	
296	9.2.1	All client based VPNs utilize industry standard technologies.	R	☐ C ☐ No ☐ N/A	
297	9.2.1	All client based VPNs and/or consolidated modem pools access utilize strong authentication which includes single use passwords.	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
298	9.2.1	All client based VPNs and/or consolidated modem pools access are controlled by a Firewall.	R	☐ C ☐ No ☐ N/A	
299	9.2.1	All client based VPNs and/or consolidated modem pools access are logged.	R	☐ C ☐ No ☐ N/A	
300	9.2.2	If directly attached modems are used, have they been approved using the exception methodology in Section 12?	R	☐ C ☐ No ☐ N/A	
301	9.2.2	Directly attached modems utilize industry standard third party authentication schema.	R	☐ C ☐ No ☐ N/A	
302	9.2.2	Use of only 'secured modems' is permitted. Uncontrolled use of modems can result in serious vulnerabilities and shall use risk mitigation measures	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
303	9.2.2	When such modems are utilized through approved exception, they meet all criteria established for client based VPN or consolidated modem pools. Including firewall access controls and single use passwords.	R	☐ C ☐ No ☐ N/A	
304	9.2.2	An accurate inventory of directly attached modems is maintained.	R	☐ C ☐ No ☐ N/A	
305	9.2.2	Other modem technologies which shall be considered include "dial/dial back", only when primary access means is down or attached only to devices which have strong authentication mechanisms.	R	☐ C ☐ No ☐ N/A	
306	9.2.2	The use of modems which are directly attached to servers, routers, switches, or other such equipment is strongly discouraged and should be prohibited by default	BP	☐ C ☐ No ☐ N/A	
307	9.3.1	When using private facility networks such as T1, DS-2, etc., whenever possible the network technologies should be always considered in lieu of communications over public transport	BP	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
308	9.3.1	Organizations should evaluate the importance of the data traversing the network and determine if encryption is appropriate to meet the necessary privacy levels (note: Use of these network technologies does not necessarily preclude the need for end to end encryption)	BP	☐ C ☐ No ☐ N/A	
309	9.3.2	Communications over the Internet must be encrypted using IPSEC or SSL.	R	☐ C ☐ No ☐ N/A	
310	9.3.2	If using endpoint authentication it has been implemented using either certificates or similar credentials.	R	☐ C ☐ No ☐ N/A	
311	9.3.2	When using Internet protocols, industry standard protocols are to be used with minimum key length of 128 bit.	R	☐ C ☐ No ☐ N/A	
312	9.3.3	When external connections are clearly identified as un-trusted, a firewall must be utilized to control communication between the external endpoint or network and the NG9-1-1 environment.	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
313	9.3.4	When applications require access from external, public transport (i.e. Internet) they have been placed on a DMZ or employ network based encryption and authentication.	R	☐ C ☐ No ☐ N/A	
314	9.4	When using Intrusion Detection / Prevention technologies they shall be positioned on internal networks at strategic locations. Note: use of IPS/IDS is not mandatory.	R	☐ C ☐ No ☐ N/A	
315	9.4	When using Intrusion Detection / Prevention technologies, their signatures must be routinely updated with processes that include well defined schedules for signature updates and emergency update protocols for high risk and zero day events.	R	☐ C ☐ No ☐ N/A	
316	9.5	When used, technologies such as VLAN, VRF, or VPN are classified as required in section 9.3 and once classified they are treated as separate networks.	R	☐ C ☐ No ☐ N/A	
317	9.5	All support equipment for virtual or logical networks shall have a management tunnel for support and monitoring.	R	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
318	9.5	All support equipment for virtual or logical networks limits user group access to the particular virtual facilities when possible.	R	☐ C ☐ No ☐ N/A	
319	9.5	Commands (like Telnet), which allow direct access between virtual facilities, are disabled or is only allowed under the highest administrative privilege supported by the device.	R	☐ C ☐ No ☐ N/A	
320	9.5	Layer 3 interactions between networks of differing security classifications are only done using a firewall or similar device.	R	☐ C ☐ No ☐ N/A	
321	9.5	User access to devices supporting multiple virtual networks should utilize an industry standard authentication and access control protocol such as TACACS or RADIUS.	BP	☐ C ☐ No ☐ N/A	

Section 11 - Network / Firewall / Remote Access Auditor:_____ Date:_____

Section 12 - Security Enhancement Technical Upgrade

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
322	4.2	Does the organization have a Security Enhancement/Technology Upgrade Policy?	R	☐ C ☐ No ☐ N/A	
323	6.7	Do the design, development, administration, and use of any computer resource, network, system, or application always enable compliance with security policies and requirements to its intended use?	R	☐ C ☐ No ☐ N/A	
324	6.7	Is incorporating security into new products, services, systems, and networks before they are deployed a priority?	R	☐ C ☐ No ☐ N/A	
325	6.7	Is a security assessment of controls and procedures conducted and documented before deployment to certify compliance with security policy and is this document retained as evidence for any future audit?	R	☐ C ☐ No ☐ N/A	
326	7.2.8	Is a full business and security assessment conducted for any new form of communications prior to it being connected to the NG 9-1-1 environment?	R	☐ C ☐ No ☐ N/A	

Section 12 - Security Enhancement Technical Upgrade

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
327	7.2.8.2	Are communication partners and the full scope of products subjected to full risk assessment?	BP	☐ C ☐ No ☐ N/A	
328	7.2.8.3.1	Are Client Software Add-ons ("plug ins") assessed for security risks?	R	☐ C ☐ No ☐ N/A	
329	7.2.8.3.1	Is client software configured to disallow auto installation of software add-on or plug-ins?	R	☐ C ☐ No ☐ N/A	
330	7.2.8.3.1	Are new add-ons or plug-ins tested prior to installation?	R	☐ C ☐ No ☐ N/A	
331	7.2.8.5	If the NG 9-1-1 Entity uses a VoIP system it does not connect to another VoIP System without securing the connection?	R	☐ C ☐ No ☐ N/A	
332	9.6.1	Network **redundancy** is considered and implemented where possible for On-Site / Local High Availability environments.	R	☐ C ☐ No ☐ N/A	

Section 12 - Security Enhancement Technical Upgrade

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
333	9.6.2	Network **diversity** is considered and implemented where possible when implementing NG9-1-1 networks.	R	☐ C ☐ No ☐ N/A	
334	9.6.2	Traffic failover between different cities and firewall sites can result in dropping sessions at the time of failure. When employing applications in a network diversity-type model, applications shall be designed to recover such events and users advised to proper "restart" procedures in case such a failover event happens	R	☐ C ☐ No ☐ N/A	

Section 12 - Security Enhancement Technical Upgrade Auditor:_____ Date:_____

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
335	10	Formalized pre and post security reviews are conducted when changes to architecture, design, or engineering of NG9-1-1 networks.	R	☐ C ☐ No ☐ N/A	
336	10	Security reviews are conducted by the NG91-1 security representative and any 3rd party vendors.	R	☐ C ☐ No ☐ N/A	
337	10	When changes to architecture, design, or engineering of NG9-1-1 network are made, a formal change control process is followed and appropriate documentation is produced and retained.	R	☐ C ☐ No ☐ N/A	
338	10	When architecture, design, or engineering are major, a team of Subject Matter Experts is assembled to review and approve the change.	R	☐ C ☐ No ☐ N/A	
339	4.2	Does the organization have a Technology Selection Policy?	R	☐ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
340	7.4.2	Is time synchronization in accordance with the NENA 04-002 NG9-1-1 Entity Master Clock standard?	R	☐ C ☐ No ☐ N/A	
341	7.4.4	Do formal documented procedures exist for any changes to computer systems and operating systems software?	R	☐ C ☐ No ☐ N/A	
342	7.4.4	Are the procedures identified in the preceding finding followed?	R	☐ C ☐ No ☐ N/A	
343	7.4.4	Is the appropriate level of authorization required and obtained prior to change?	R	☐ C ☐ No ☐ N/A	
344	7.4.4	Does the System Administrator control software changes that affect the operation of an application, operating system, or utilities?	R	☐ C ☐ No ☐ N/A	
345	7.4.4	Does the System Administrator control updates and upgrades that could affect user response, machine performance or operations, security, or system availability?	R	☐ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
346	7.4.4	Has a detailed audit trail of all modifications to network hardware and software been created, retained, and reviewed at least annually?	R	☐ C ☐ No ☐ N/A	
347	7.4.4	Are records of all system/application changes kept at least one year or the last major upgrade whichever is longer?	R	☐ C ☐ No ☐ N/A	
348	7.4.4	Do System Controls identify accountability for all program changes to a specific programmer and approving manager?	R	☐ C ☐ No ☐ N/A	
349	7.4.4	Excepting reporting procedures are built into the system software to detect computer program, communications and operations failures. .	R	☐ C ☐ No ☐ N/A	
350	7.4.4	Are error checking and validation controls are present in software?	R	☐ C ☐ No ☐ N/A	
351	7.4.4	Current complete backups are ALWAYS present prior upgrades to provide recovery capability in the event of system problems due to the changes?	R	☐ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
352	7.4.4	If System Administration or Maintenance is outsourced all records kept by such agencies are available to the NG 9-1-1 Entity?	R	☐ C ☐ No ☐ N/A	
353	7.4.5	Have procedures been instituted to verify and document that the business hardware and software are currently supported by the manufacturer or supplier that advisories are issued and fixes are made available for any newly discovered security vulnerability?	R	☐ C ☐ No ☐ N/A	
354	7.4.5	Are Temporary Fixes applied when Permanent Fixes are not yet available and are Permanent Fixes applied promptly when they become available?	R	☐ C ☐ No ☐ N/A	
355	7.4.5	A process is in place which ensures all applicable Permanent fixes are installed and Temporary Fixes cannot become disabled until Permanent Fixes have been installed?	R	☐ C ☐ No ☐ N/A	
356	7.4.5	Are all Permanent or Temporary fixes tested prior to using them in a production environment?	R	☐ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
357	7.4.6	Servers, workstations, desktops, or laptops shall be hardened utilizing recognized 'Best Practices for Operating System Hardening' like the National Institute For Standards and Technology (NIST) Guidelines or ISO 2700*x* standards?	R	☐ C ☐ No ☐ N/A	
358	7.4.6	All unused services are disabled and end users do not have local administrator rights?	R	☐ C ☐ No ☐ N/A	
359	7.5.2	Has the entity identified all 'single point of failure' items for their system and have the alternate strategies been planned and documented?	R	☐ C ☐ No ☐ N/A	
360	7.5.2	Is a plan in place to distribute the 'downtime window' if possible?	R	☐ C ☐ No ☐ N/A	
361	7.5.2	Is equipment managed and monitored so if one element is down the entity and management are notified?	R	☐ C ☐ No ☐ N/A	
362	7.5.3	Is 'geographic redundancy' available. If so, are procedures in place for activation, use, and testing of the alternate site. Are the results of testing documented	R	☐ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
363	7.5.3	Are the results of testing of failover procedures documented?	R	☐ C ☐ No ☐ N/A	

Section 13 - Technical Solutions Standards Auditor:_____ Date:_____

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
364	4.2	Does the organization have a Wireless Policy? (Auditor Guidance: if no wireless technologies are in place, then this finding, and all subsequent findings is not applicable All requirements of this document also apply to communications in the 4.9G Hz band)	R	☐ C ☐ No ☐ N/A	
365	6.4.6.1	Default router management passwords have been changed and is treated as an Administrator level password for syntax, history, and periodically changed?	R	☐ C ☐ No ☐ N/A	
366	6.4.6.1	Router management over wireless link is disabled Router management uses an encrypted protocol?	R	☐ C ☐ No ☐ N/A	
367	6.4.6.1	The SSID has been changed from the Default value to an identifier not easily associated with the NG 9-1-1 or easily guessed	R	☐ C ☐ No ☐ N/A	

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
368	6.4.6.1	SSID broadcast is disabled?	R	☐ C ☐ No ☐ N/A	
369	6.4.6.1	Wireless encryption is enabled WPA or greater is used? (Auditor Guidance: WEP is not allowed)	R	☐ C ☐ No ☐ N/A	
370	6.4.6.1	The TKIP passphrase is non-trivial and meets the requirements of this document?	R	☐ C ☐ No ☐ N/A	
371	6.4.6.1	The rekey maximum is no greater than 3600 seconds?	R	☐ C ☐ No ☐ N/A	
372	6.4.6.1	The WIFI LAN is dedicated to the NG 0-1-1 entity and not shared with any other entity?	R	☐ C ☐ No ☐ N/A	

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
373	6.4.6.1	Media Access Control (MAC) address filters are enabled and MAC Filter List is reviewed at least monthly and immediately after a machine is retired from the network?	R	☐ C ☐ No ☐ N/A	
374	6.4.6.1	Ad hoc modes are disabled?	R	☐ C ☐ No ☐ N/A	
375	6.4.6.1	Users should be authenticated to the wireless LAN using a two factor mechanism or emerging authentication standards like 802.1x?	BP	☐ C ☐ No ☐ N/A	
376	6.4.6.1	The WIFI LAN should be separated from other networks by a firewall which limits access to and from the wireless network on an exception only basis.	BP	☐ C ☐ No ☐ N/A	
377	6.4.6.1	Use of Intrusion Detection Systems (IDS) is encouraged on WIFI LANs	BP	☐ C ☐ No ☐ N/A	
378	6.4.6.1	Maximum encryption key lengths supported by the device should be utilized	BP	☐ C ☐ No ☐ N/A	

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
379	6.4.6.1	The WIFI LAN hardware should utilize a third party authentication service for management(such as TACAS, Radius) when supported	BP	☐ C ☐ No ☐ N/A	
380	6.4.6.1	The default SSID channel should be changed from its default value	BP	☐ C ☐ No ☐ N/A	
381	6.4.6.1	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	BP	☐ C ☐ No ☐ N/A	
382	6.4.6.1	DHCP should be disabled and require static IP Addresses for connected devices. If DHCP must be used the DHCP scope(range of addresses) should be kept to a minimum	BP	☐ C ☐ No ☐ N/A	
383	6.4.6.1	The WIFI LAN should utilize a Network Access Control technology to ensure proper patching and malicious software screening is performed on all LAN assets. At minimum, use of a rogue machine device detection capability is strongly recommended.	BP	☐ C ☐ No ☐ N/A	

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
384	6.4.6.2	Bluetooth shall not be used for backup of any medium or device which contains sensitive (internal data only) or greater data.	R	☐ C ☐ No ☐ N/A	
385	6.4.6.2	If Bluetooth is used is shall be configured to require device identifiers.	R	☐ C ☐ No ☐ N/A	
386	6.4.6.2	Presence of frequency hopping, phase shifting, device serialization, or other technologies alone shall not satisfy encryption or identification requirements	R	☐ C ☐ No ☐ N/A	
387	6.4.6.2	Bluetooth wireless networks should be avoided, where possible, including wireless headsets and other human interface devices such as mice and keyboards	BP	☐ C ☐ No ☐ N/A	
388	6.4.6.3	Does the entity use the 4.9 MHz band spectrum licensed by the FCC?	R	☐ C ☐ No ☐ N/A	
389	6.4.6.3	If the 4.9 MHz band is used are all communications encrypted and all authentication, authorization, and accountability policies complied with?	R	☐ C ☐ No ☐ N/A	

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
390	6.4.6.3	If the 4.9 MHz band is used a Firewall is deployed at the network boundary	R	☐ C ☐ No ☐ N/A	
391	6.4.6.3	All communications on the 4.9G Hz band should be encrypted?	BP	☐ C ☐ No ☐ N/A	
392	6.4.6.3	Authentication, authorization, and accountability should be maintained.	BP	☐ C ☐ No ☐ N/A	
393	6.4.6.4	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	R	☐ C ☐ No ☐ N/A	
394	6.5	Does the NG 9-1-1 entity require contracting agencies to hold specific or certain certifications to prove compliance with this requirement?	R	☐ C ☐ No ☐ N/A	

Section 14 - Wireless Security

Audit Item Number	NG-SEC Standard	Audit Area	Compliance Type	Compliance Finding	Comments
395	6.5	Entities responsible for system and security administration (including those contracted to do such tasks) employ individuals who have received current security training on their assigned systems.	R	☐ C ☐ No ☐ N/A	
396	6.5	All Public Safety employees receive complete security awareness training as established by each Public Safety Organization on an annual basis?	R	☐ C ☐ No ☐ N/A	

Section 14 – Wireless Security Auditor:_____ Date:_____

Auditor Comments:

Auditor Notes

Auditor Instructions:

4 Appendices

Appendix A: Exception Risk Approval / Mitigation Timeframe Table

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

5 Recommended Reading and References

It is recommended that the user of this document be very knowledgeable with:

- NENA 75-001 - NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)