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

Abstract: Establish the minimal guidelines and requirements for the protection of NG9-1-1 assets or elements within a changing business environment.

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

NENA-STA-040.2-2024 (originally 75-001, v1)
DSC Approval: September 10, 2024
PRC Approval: September 26, 2024
NENA Board of Directors Approval: October 28, 2024
ANSI Approval: November 4, 2024
Next Scheduled Review Date: November 4, 2027

Prepared by:
National Emergency Number Association (NENA) Systems Security & Resiliency Committee, Security for NG9-1-1 Working Group

1 Executive Overview

The purpose of this document is to establish the minimal guidelines and requirements for the protection of Next Generation 9-1-1 (NG9-1-1)[1] assets or elements within a changing business environment.

This document:

- Identifies the basic requirements, standards, procedures, or practices that 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 recommends using National Institute of Standards and Technology (NIST) NIST 800-30 Rev 1, *Guide for Conducting Risk Assessments* [13] in the case of non-compliance to these guidelines.

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

- 9-1-1 Authorities
- Public Safety Answering Points (PSAPs) and Emergency Communication Centers (ECCs)
- NG9-1-1 Emergency Services Internet Protocol (IP) network (ESInet) providers
- Next Generation 9-1-1 Core Services (NGCS) Functional Element (FE) providers
- Telecommunications Service Providers (regardless of access, carrier, service, technology, or media type used)
- NG9-1-1 vendors, solution providers, application providers, integrators, equipment hardware and software providers, etc.
- Any contracted service that performs functions or services that require securing NG9-1-1 assets, data, and staff.

A NG9-1-1 system consists of, but is not limited to, various systems, applications, databases, services, as well as those individuals who use, design, have access to, interface with, or are responsible for NG9-1-1 assets. A cybersecurity program must be developed and maintained when operating a NG9-1-1 system. The cybersecurity program establishes the numerous cybersecurity roles, responsibilities, and obligations for a NG9-1-1 system.

Section 3.4 Roles & Responsibilities defines the minimum roles and responsibilities required to manage each NG9-1-1 system or entities component thereof. Additional roles and responsibilities will be defined by each entity as needed.

This document outlines a framework to assist 9-1-1 authorities in developing a robust cybersecurity plan. This document is expected to help build and strengthen cybersecurity programs by focusing on NG9-1-1 security through policy management, security and risk management and operations, data security, and operations.

[1] Assets consist of but not limited to hardware, software, and/or data that belongs to a NG9-1-1 Entity.

Table of Contents

Table of Figures

Table of Tables

NENA
STANDARD DOCUMENT
NOTICE

This Standard Document (STA) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. As an industry Standard it provides for interoperability among systems and services adopting and conforming to its specifications.

NENA reserves the right to revise this Standard 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,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations 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, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license is granted, whether expressed or implied. 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.

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 changes 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

2 Document Conventions

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally-available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at https://www.nena.org.

2.1 Document Terminology

This section defines keywords, as they should be interpreted in NENA documents. The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

1. MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute) requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "must" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF RFC 2119 [2].

2.2 NENA Intellectual Property Rights (IPR) and Antitrust Policy

NOTE – The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, NENA takes no position with respect to the validity of any such claim(s) or of any patent

rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at https://www.nena.org/ipr.

Consistent with the NENA IPR and Antitrust Policy, available at https://www.nena.org/ipr, 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

2.3 Reason for Issue/Reissue

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

Document Number	Approval Date	Reason For Issue/Reissue
NENA 75-001	February 6, 2010	Initial Document
NENA 75-001.1	May 25, 2015	Update webpage links
NENA-STA-040.2-2024	November 4, 2024	Major rewrite to accommodate new technologies and practices that have emerged since the initial document was published.

3 Technical Description

3.1 Overview

NENA provides the technical and operational framework for establishing cybersecurity standards for NG9-1-1 within this document. The objective of the Next Generation 9-1-1 Security (NG-SEC) standard is to envelop the mechanisms, processes, and functions that utilize an NG9-1-1 system to send and receive traffic for emergency services. The technical areas contained in this Standard enable the development of a common cybersecurity posture for all NG9-1-1 systems.

The NENA-STA-040.2-2024 standard has been grouped into three domains that cover specific security features, functions, or processes. When these domains and their

subcomponents are combined, they work together to help build a defense in depth approach to cybersecurity. Figure 3-1 NG-SEC Framework shown below graphically depicts the security domains that are discussed in this document.

While this document focuses primarily on NG9-1-1 security requirements, many of the concepts described herein can also be applied to legacy E9-1-1 systems as well.

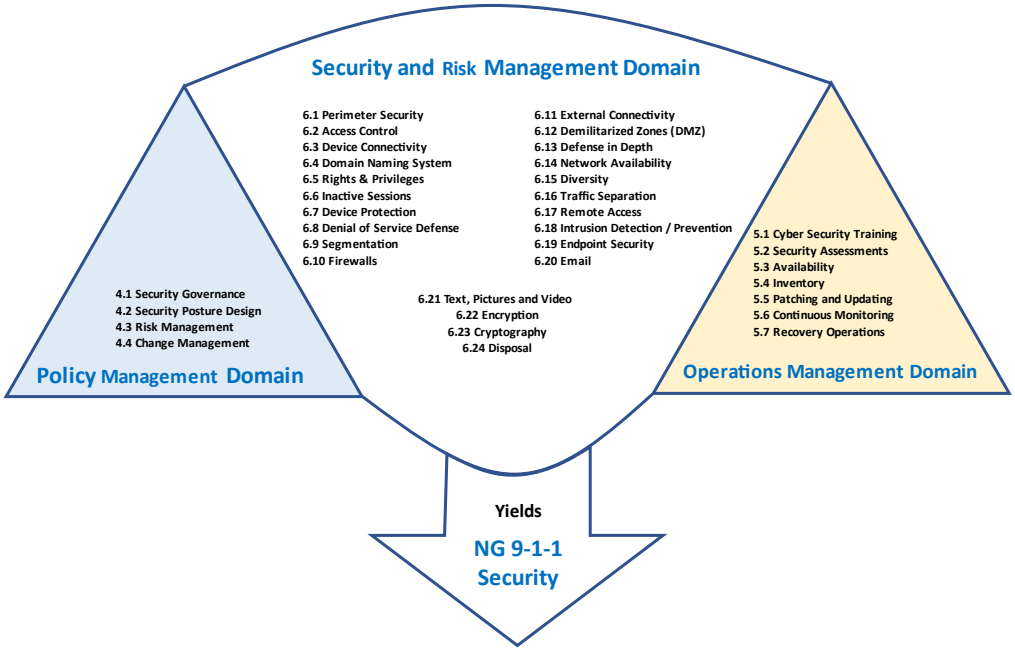

Figure 3-1 NG-SEC Framework

The objectives of this NG-SEC standard are to aid all entities managing components of a NG9-1-1 system. This is accomplished by the:

Policy Management Domain

The Policy Management Domain focuses on the documentation of all guidelines, rules, and expectations of security by the 9-1-1 Authority with oversight responsibility for the system. This domain contains the establishment of security governance, posture, and policies for the entire system.

Operations Management Domain

The Operations Management Domain focuses on the areas that apply to the functional and non-functional implementation of components, services, and systems that protect the network(s) used for a NG9-1 1 system. This domain contains the implementation of tools, services, and applications that serve to detect, monitor, and manage the system.

Security and Risk Management Domain

A Security and Risk Management Domain focuses on the areas that apply to the functional and non-functional implementation of components, services, and systems that protect the NG9-1-1 system. This domain contains the deployment of such things as physical security, firewalls, system hardening and intrusion protection.

3.2 Statement of Compliance

The information contained within this document helps provide the minimal protection necessary for NG9-1-1. This is accomplished through developing and implementing detailed security requirements, standards, procedures, and practices.

- Non-compliance with security requirements, standards, procedures, and practices SHALL be documented to identify security vulnerabilities, determine associated criticality, and establish a compliance action plan and/or risk acceptance.
- Unresolved non-compliance SHALL require documented risk acceptance as described in Section 4.3 Risk Management.

3.3 Severity Categories

A cybersecurity audit is used for determining whether entities comply with the security requirements stated herein. Security categories are based on the potential impact should certain event(s) occur and are used in conjunction with vulnerability and threat information in assessing the risk and assigning priority.

- A cybersecurity audit SHALL follow, at a minimum, the severity categories as defined in NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* [3].

3.4 Roles & Responsibilities

Safeguarding NG9-1-1 assets, both physical and digital, is the responsibility of everyone. An effective security program requires many different roles and responsibilities. These may be within or external to a NG9-1-1 Entity. The following responsibilities define the minimum required. An Entity may use a different name or title as long as the responsibility defined is assigned to an individual. For example, an Entity may have an IT Manager who is assigned the Security Manager responsibilities and not use the title of Security Manager.

- Every individual within a NG9-1-1 Entity SHALL be informed of their on their respective roles and responsibilities as they apply to NG9-1-1 and included in the security 'mindset' of that Entity, and it SHALL be documented.
- The following responsibilities SHALL be fulfilled:
    - **Security Manager:** Executive or other department manager with the authority and responsible for the security of the Entity. This individual, or

their designated representative, SHALL define security policy as it relates to all components, physical and/or digital, of a NG9-1-1 Entity as a whole.

- **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, declassifying, and disposing of data for which they are the Data Owner for on a NG9-1-1 system. All data, local or remote, in a NG9-1-1 system SHALL have a Data Owner. It does not need to be the same individual for all data. Each Data Owner is responsible for helping a NG9-1-1 Entity understand the importance of the data they are responsible for in order to establish the necessary level of protection.
- **Data Custodian:** Responsible for ensuring that all security measures required for data, or subset of data, are implemented, adhered to, and maintained. All data, local or remote, at rest and in transit, in a NG9-1-1 system SHALL have a Data Custodian. It does not need to be the same individual for all data.
- **Data User:** Responsible for complying with all security policies and procedures for NG9-1-1 data. Any authorized individual who accesses NG9-1-1 data is a Data User. For example, a Dispatcher is a Data User in that they 'use' 9-1-1 call data to perform their daily tasks.
- **Security Audit Manager:** Responsible for ensuring that periodic audits of a NG9-1-1 system are completed, and all findings are addressed. Audits may be performed by internal or external resources. A risk assessment form SHOULD be conducted for all findings.

Some roles may be fulfilled in a shared manner as long as there is an individual accountable for each responsibility.

4 Policy Management Domain

A NG9-1-1 system environment with vendors, contractors, and suppliers for supporting resources and services should also include security control requirements (management, operational, technical) through a contract. The requirements applied to the entire supply chain resource environment will support an information security posture within a system managed NG9-1-1 environment.

- The contract SHALL clearly detail the roles and responsibilities of each party and SHOULD include applicable security reviews, assessments, and/or audits to ensure the protection of all relevant information, systems, services, or other resources. Some roles and responsibilities include, but are not limited to, administration, maintenance, patching, management, and recovery.

- When outsourcing data or systems that contain data, the contract SHALL clearly define who owns that data.
- Contractors, suppliers, and subcontractors SHALL protect that data in accordance with the terms and conditions of applicable contractual agreements between the contractor or supplier and a NG9-1-1 Entity.
- In addition, it SHALL be the responsibility of all contractors, suppliers, and subcontractors to comply with applicable federal, state/province/territory, and local acts, statutes, and regulations that relate to the control and authorized use of information and information resources.

4.1 Security Governance

4.1.1 Senior Management

NG9-1-1 presents new threats and risks that were not prevalent before transitioning to IP technology. Senior management is responsible for providing support for the creation and maintenance of a highly effective security posture. Security cannot be made someone else's responsibility; everyone, and especially management, shall be involved and vigilant. Creating a senior management statement of policy is crucial to documenting the importance of the technical assets and resources within an NG9-1-1 Entity. This can be done through a commitment to exercise due care through the definition and management of acceptable technical, functional, and operational level standards, procedures, and measures.

- Senior management SHALL create and model a culture of security as outlined in this document.
- The Senior Management SHALL, at a minimum:
  - Provide documentation defining the security goals and objectives for a NG9-1-1 Entity.
  - Provide the necessary resources to accomplish the security goals and objectives for a NG9-1-1 Entity.
  - Assign the roles and responsibilities for a NG9-1-1 Entity.
  - Retains overall responsibility for a NG9-1-1 Entities security program.
  - Instill and model a NG9-1-1 Entity wide security mind set.

4.1.2 Policies

Policies provide documentation on how a NG9-1-1 Entity defines what can and cannot be done. They set the overall tone and guidelines for security.

A cybersecurity policy is a documented strategy defining an Entities' purpose, scope, roles, responsibilities, management commitment, coordination, and compliance in relation to securing NG9-1-1. Cybersecurity policy is the sum-total of security polices vital to a security program.

It is recommended that each policy be a separate standalone document, but they may be combined provided that each area is addressed. All policies should be reviewed and updated periodically to cover emerging technologies, techniques, and processes.

A NG9-1-1 Entity SHALL, at a minimum, have the following policies:

- **Acceptable Use Policy:** This policy defines what users may or may not do on or with NG9-1-1 system equipment, software, and applications.
- **Auditing and Assessment Policy:** This policy defines the frequency and scope of security audits and assessments.
- **Authentication/Password Policy:** This policy defines authentication and password requirements for a NG9-1-1 Entity.
- **Change Management Policy:** This policy defines the process by which changes can be made to a NG9-1-1 system. This policy defines the documentation and authorization requirements for planned and unplanned changes. It also defines what routine changes are authorized along with any requirements for them.
- **Cybersecurity Incident Response Policy:** This policy defines actions and procedures to take in the event of a cybersecurity incident as well as how and when to bring in outside assistance.
- **Data Protection Policy:** This policy defines the data classification levels, how that data is to be labeled, handled, stored, managed, and disposed of. The policy will define how third-party data will be handled and will cover public records requests.
- **Equipment Disposal Policy:** This policy defines how equipment will be disposed of.
- **Endpoint Protection Policy:** This policy defines the security controls and patch management for each type of device.
- **Hiring Practices Policy:** This policy defines how employees will be vetted and trained. Their training needs to cover security policies and inclusion in the Security Awareness program.
- **Physical Security Policy:** This policy defines physical access and theft prevention requirements.
- **Procurement Policy:** This policy defines how technical items are purchased in relation to identifying and mitigating security risks (e.g., supply chains, software, hardware) while complying with internal security guidelines and requirements [5].
- **Remote Access Policies:** This policy defines authorized methods for all external remote connections to NG9-1-1.
- **Risk Management Policy:** This policy defines how risk is assessed resulting from threats to the confidentiality, integrity, and availability of NG9-1-1 assets.
- **Security Awareness Training Policy:** This policy defines the frequency and core topics of the Entities security awareness training.
- **Security Monitoring Policy:** This policy defines logging, endpoint monitoring, and traffic monitoring and how often that information will be reviewed.

4.1.3 Procedures

Best practices are used to create procedures for maintaining a secure environment and handling physical and cybersecurity events. It is important to document procedures within a NG9-1-1 Entity as they are an important part of the security strategy and help create consistency and accountability. Procedures help establish an authorized and approved process to complete tasks that comply with the Entities' security posture. Many of these tasks are repetitive in nature. Some only happen periodically and hence it becomes even more important that the correct process be documented as it is often not the same individual performing the task. Some examples of processes that are needed include creating new user accounts, setting up remote access for a vendor, and recovering a lost system or data. As an organization's security policies evolve to handle changing technologies and threats, it will become necessary to update existing procedures or create new ones.

- A Standard Operating Procedure (SOP) that details the technology and tasks related to maintaining a secure environment for a NG9-1-1 Entity SHALL be established.
- SOPs SHALL be developed, maintained, periodically updated, and utilized for all identified tasks.

4.1.4 Information Classification and Protection

Information classification is the cornerstone for evaluating and protecting assets, both physical and digital, owned and used by a NG9-1-1 Entity. Information is categorized based on the sensitivity, applicable policies, and/or legal and statutory requirements. Third-party data may also have classification parameters that must be adhered to such as the Criminal Justice Information Services (CJIS) data.

Data has three states: Data at rest, data in use, and data in transit. Proper protections and handling relative to the data's classification in each state needs to be maintained. A possible method for controlling access to data is through Data Rights Management (DRM) and Data Loss Prevention (DLP). Section 5.6 in the NENA i3 Standard for Next Generation 9-1-1, NENA-STA-010.3-2021 [6] outlines authorization and DRM. DRM is used to ensure that only intended recipients can view protected files. DLP tracks the flow of data within an organization and can apply policies that affect what can be done with the data.

NENA i3 specifies the XACML based mechanism to implement DRM policy that is enforceable by the NGCS and PSAP systems that mandate its use.

4.1.4.1 Information Classification Policies

Each NG9-1-1 Entity is responsible for establishing the information classification parameters for its respective operations. This information will be defined in the Data Protection policy. This policy defines how data is handled for internal use, external use, and for public records requests.

4.1.4.2 Roles and Responsibilities in Information Classification and Protection

The following outlines the minimum roles and responsibilities for information classification and protection. An important concept in limiting access to information is called the principle of least privilege. The principle of least privilege is the practice of only providing the minimum permissions necessary for the user's job. These permissions are for devices, data, functionality, and/or any other resource. This means a user can only log onto systems, perform actions, and/or read/write/modify/delete data necessary to accomplish their job and nothing else.

4.1.4.3 Data Owner

When an employee, vendor, contractor, agent, or service provider is designated as responsible for a set of data, they become the Data Owner.

The Data Owner SHALL:

- Assess the risk associated with the loss of data for which they are the Data Owner.
- Judge the value of the data and assign the proper classification level according to the Data Protection Policy.
- Periodically review the classification level for all data for which they are the Data Owner to determine if the status should be changed.
- Communicate access and control requirements to the Data Custodian and users.
- Authorize appropriate level of access using the principle of least privilege for those individuals who have a demonstrated business need for access (read/write/delete).
- Ensure that the required security controls are in place to mitigate the risk to data integrity, confidentiality, and availability.
- Conduct, at a minimum, an annual audit of all data for which they are the Data Owner.
- Monitor safeguard requirements to ensure that information is being adequately protected.

4.1.4.4 Data Custodian

A Data Custodian is responsible for protecting the data they are responsible for according to the rules and regulations established by the Data Protection Policy.

Being granted access to data does not imply or confer authority to grant other users access to that data. This is true whether the data is electronically held, printed, hardcopy, manually prepared, copied, or transmitted.

- When an employee, vendor, contractor, agent, or service provider retains data, they SHALL become a custodian for that data.
- A Data Custodian SHALL:
  - Ensure data is used as authorized and only for the purpose intended.
  - Ensure access by authorized users with a demonstrated business need.

- Maintain the integrity, confidentiality, and availability of the data for which they are the Data Custodian.
- Comply with information classification and protection policies on retention and disposal of records and data.
- Ensure required safeguards are being used for processing equipment, information storage, backup, and recovery.
- Ensure the data is used in an authorized secure processing environment that can adequately protect the integrity, confidentiality, and availability of information.
- Periodically review data access to ensure that it is only authorized users have access and it is being used for the purpose intended.

4.2 Security Posture Design

Design, development, administration, and use of any computer resource, network, system, or application should always enable compliance with all security policies and requirements applicable to its intended use. Incorporating security into new products, services, systems, and networks before they are deployed needs to be a priority.

Note that PSAPs and other 9-1-1 Authorities are usually unable to assert fine grain controls on data stored within purchased applications and must rely on the mechanisms those applications provide.

4.2.1 Security Assessment Documentation

Security policy and requirements, and/or risk assessments should be a consideration in any development or product realization process. Security policy and requirements, and/or risk assessments should be a consideration in any development or product realization process. A security assessment of controls and procedures must be conducted and documented for all resources before deployment to certify compliance with security policy. The security review documentation should be retained as evidence for any future audit.

- All components of a NG9-1-1 system SHALL be covered by a documented security assessment. If desired, a security assessment can cover multiple components rather than an assessment for each individual component.

4.2.2 Information Classification Guidelines

All data within an NG9-1-1 Entity has a value and should be considered an asset across all functional and operational units. Therefore, all data needs to be protected just like any other physical or operational asset. NG9-1-1 systems use a standardized Data Rights Management system defined in STA-010 [6] which allows each interface, each data object and/or element in a data object to be restricted by a standard data rights management policy created by an agency. Other computerized systems may have different data rights management systems. Where data is manually managed, data must be classified as

described below and manual policies created that control access to data by classification. This section is intended to serve as a guideline to classifying and accessing data not managed by a more sophisticated data rights management system. This section is intended to serve as a guideline to classifying and accessing data. NG9-1-1 Entities should ensure they comply with all applicable laws and regulations. There are some exemptions to data protection when used for emergency services since the drawbacks of disclosing personal data are outweighed by the benefit for the emergency caller.

Data must be protected at a level that addresses the confidentiality, integrity, and availability of that data. To better utilize limited resources, it is more efficient to apply costly controls to data with a higher level of sensitivity than to all data across the board. Data can be grouped to help facilitate classification levels. The classification level is determined by the highest level of sensitivity of data contained within a group. Classification levels help ensure that the data is protected appropriately and that the appropriate level of security controls and measures are being utilized.

4.2.2.1 Classification Levels

NOTE: Information that is proprietary to another Entity agency must be obtained legally with the agreement of the other Entity and in compliance with the appropriate code of conduct. Information must be classified using the highest applicable classification level based on the sensitivity of the information as described below.

WARNING: There may be copyright, local legislation, or other legal requirements that apply to some collections of data. Check with your local legal counsel for clarification.

- The Data Protection Policy SHALL specify the different classification levels of data not covered by a more comprehensive data rights management system for the Entity. In this section, the term "classified data" means data not controlled by a data rights management system.
- The Data Protection Policy SHALL define which classifications levels the Entity believes are not subject to the Freedom of Information Act (FOIA) [7] or similar laws [8] [9].
- All classified data SHALL be assigned a classification level according to the highest sensitivity of any information in that data set.
- 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 a 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.
- Access to sensitive information SHALL be reviewed at least annually.

The following are the minimum recommended classification levels for classified data for a NG9-1-1 Entity.

4.2.2.1.1 Public

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

Description

- Information for which there is no value in keeping secret.
- 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. This does not imply that the information must be made accessible from the public domain, only that it is available in accordance with local regulations.

Examples of Public Information

- Guidance for ordering products and services (i.e., Vendor Product Briefs, RFPs).
- Publicly available contact information (e.g., email, text, social media, or listed phone number to the Police Department).

4.2.2.1.2 Sensitive (Internal Use Only)

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

- Release of Sensitive (Internal Use Only) Data/information SHALL be documented when released.

Description

- Information that is sensitive and not intended for public disclosure, whose value could be diminished if publicly disclosed.
- Information that could be valuable to create unintended obligations or liabilities if revealed.
- Information that is intended only for employees or authorized contractors.

Examples

- Internal directory entries excluding fields specifically identified in other classification levels.
- General Process and Operational information.
- Service Descriptions.

- Internal communications and instructions.
- Policies, standards, and guidelines.
- Data relating to internet usage.

4.2.2.1.3 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.

Description

- Information that the data owner determines should be shared only among those with a clear need to know.
- Information that, if revealed to unauthorized individuals, could present an increased risk of compromising systems, disrupting the day-to-day operations of a NG9-1-1 Entity, or facilitating fraud.
- Not intended for public release.

Examples

- Strategic operational plans including backup sites, fuel depots, etc.
- Audit information and incident reports.
- Network information such as logs, authentication credentials (passwords and pins), network diagrams, source code, firewall rules, and configuration files.
- Research and development information including studies, designs, and development plans for new or improved products, services, or processes.
- Attorney-Client Privileged information.
- Customer Proprietary Network Information (CPNI) as described in the US Telecommunications Act of 1996.
- Security scans and security testing results.
- 9-1-1 call data (e.g., caller's name, callback number, location, timestamps).

4.2.2.1.4 Sensitive (Most Sensitive Information)

- Most Sensitive Information SHALL only be shared 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.

Description

- Information that has a legal requirement to be protected from loss or unauthorized disclosure. Notification of loss or unauthorized disclosure of this data is often required.
- Information that, if made public, could expose NG9-1-1 Entities to the risk of physical harm, compromise of undercover operations, fraud, identity theft, etc.

Examples

- Nationally and/or State Issued Identification Number. This includes SSN, driver's license number, visa, and/or passport values.
- Full Date of Birth (DOB).
- Biometric Data. These are recordings of an individual's physical and/or behavioral characteristics and are often used for authentication purposes. Some examples include fingerprints, palm scan, and face scan.
- Medical Information.
- Background Check Data.
- Private Keys. These are digital keys used for encryption, authentication, or validation. An example is the private key used in an electronic signature used for validation.
- Personal Identification Numbers, passwords, or passcodes. Used for authentication and/or access to a system, information, or service.
- Stored password hint answers.
- Information obtained from NCIC (National Crime Information Center) or similar agencies in other countries. This falls under CJIS. NCIC is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen property, 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.

4.2.2.2 Federal Information Classification Programs

There are national level compliance requirements for certain types of data in most countries. Some types of data may have other / additional regulatory requirements. There also may be local regulations that specify how certain types of data must be handled. NG9-1-1 Entities will need to evaluate all requirements in relation to the data owned or in custody of. The following are some of the U. S. Federal regulations that may apply to NG9-1-1 Entity data, as an example.

4.2.2.2.1 Protected Critical Infrastructure Information (PCII)

Congress created the Protected Critical Infrastructure Information (PCII) Program under the Critical Infrastructure Information (CII) Act of 2002 to protect private sector infrastructure information voluntarily shared with the government for the purposes of homeland security. The 6 Code of Federal Regulations (CFR) part 29, *Procedures for*

Handling Protected Critical Infrastructure Information; Final Rule, published in the Federal Register on September 1, 2006, established uniform procedures on the receipt, validation, handling, storage, marking, and use of CII voluntarily submitted to the Department of Homeland Security (DHS).

The protections offered by the PCII Program enhance the voluntary sharing of CII between infrastructure owners and operators and the government. The PCII Program protections provide homeland security partners confidence that sharing their information with the government will not expose sensitive or proprietary data.

Information on PCII and training resources can be found at "Protected Critical Infrastructure Information (PCII) Program" [10].

4.2.2.2.2 Customer Proprietary Network Information (CPNI)

In the Telecommunications Act of 1996, Congress provided for the protection of Customer Proprietary Network Information (CPNI) and imposed an affirmative obligation of confidentiality for that information. The law defines CPNI (in 47 U.S.C. § 222(h)(1)) as:

A. Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
B. Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

The Federal Communications Commission (FCC) is responsible for implementing and enforcing the Communications Act, including the CPNI provision. The FCC has promulgated several rules and conducted several inquiries interpreting and applying the CPNI provisions since the law was passed. The FCC has made clear that both telecommunications carriers and voice over IP carriers can only release customer information to third parties after obtaining opt-in consent from customers. This includes when a carrier shares CPNI information with a joint venture partner or independent contractor for marketing purposes. However, only opt-out consent is required when telecommunications carriers share CPNI with their affiliates for communications-related purposes.

The FCC has also enforced additional disclosures and certification requirements. First, carriers are required to contact law enforcement and customers when a customer's CPNI has been breached. Law enforcement agencies can delay customer notification. Second, carriers must require password protection for online customer accounts. Customers can get access to their CPNI over the phone with a password, or customers can obtain the information in person with a valid photo ID. Carriers are also required to immediately notify customers of changes to their online account. Finally, carriers are required to provide

annual updates that add up the total number of CPNI complaints it receives from customers and any action that carriers have taken against data brokers.

4.2.2.2.3 Personally Identifiable Information (PII)

PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

4.2.2.2.4 Health Insurance Portability and Accountability (HIPAA)

Health Insurance Portability and Accountability Act of 1996 (HIPPA) [11] is a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers. Developed by the Department of Health and Human Services, these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule. HIPAA took effect on April 14, 2003.

HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information.

4.2.2.3 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.

4.2.2.4 Receipt of Sensitive Information

Sensitive information received from external parties should 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). If the sensitivity level can’t be determined, use the default classification as specified above. Some data may be covered

by a nondisclosure agreement and should be treated accordingly, subject to applicable to local laws and regulations.

- External party Sensitive Data[2] SHALL be safeguarded in the same manner as like data for the Entity and classified as such.

4.2.2.5 Protecting Sensitive Information

- To protect NG9-1-1 Entity data, policies SHALL define how each classification level of classified data is to be handled and protected relevant to the three states of data defined below.

Data must be treated as a critical component of the Entity and NG9-1-1 system.

Data within a network can be defined in three states of operation. The recognition of the three states is important to ensure that the security performed for each state is maintained and aligned with the overall security plan. All data must be handled with due care and due diligence regardless of the defined state as described below.

4.2.2.5.1 Data at Rest (Stored Data)

This encompasses, but is not limited to, data on disks, tapes, CDs/DVDs, USB thumb drives, memory cards, cloud-based storage, or other such media.

- Personally owned storage devices (i.e., user owned USB thumb drives, memory card, phones) SHALL **NOT** be used. Entity-owned and approved storage devices such as USB thumb drives, memory cards, CDs/DVDs, MAY be used based on the NG9-1-1 Entity's Data Protection Policy.
- Protection of Sensitive Data at rest SHALL be defined in the Data Protection Policy.
- The integrity of data at rest SHALL be maintained in a manner that assures that no unauthorized modifications or changes are made to the data.
- Disk encryption (full/partial) for Sensitive Data SHALL be defined in the Data Protection Policy. Storing Sensitive Data on CDs/DVDs should be avoided.
- Destruction and/or disposal procedures for Data SHALL be defined in the Disposal Policy.

4.2.2.5.2 Data in Transit (or in motion)

This is data that is being transferred from one location to another like pulling information from a Computer Aided Dispatch (CAD) database or a CJIS database.

- Sensitive Data requires encryption as defined in NENA-STA-010.3 [6] and SHALL be defined in the Data Protection Policy.

[2] Sensitive Data is information that needs to be protected from unauthorized access or modification.

4.2.2.5.3 Data in Use

This is data that is in use like when viewing a CAD display or viewing a printed or electronic personnel file.

- Data in use SHALL be safeguarded from unauthorized disclosure.
- The protection of Sensitive Data SHALL be defined in the Data Protection Policy. Additional sections for the protection of data may be included in the Data Protection Policy or separate policies such as a Clean Desk policy and Print Policy.
- NG9-1-1 Entity personnel SHALL ensure that re-used storage media is "clean" (i.e., it 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.

4.2.2.6 Safeguarding Sensitive Electronic Information

Where data marked Sensitive (Internal Use Only), Sensitive (Restricted), and Sensitive (Most Sensitive Information) is stored on removable or portable media (such as USB flash drives, thumb drives, memory sticks, external hard drives, or CDs), and/or mobile computing devices, 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).
- SHALL be kept in the direct supervision of the custodian when traveling on public transport (e.g., not be placed in taxi trunk/boot, bus hold/baggage storage, checked-in on airplane).

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

- In NG9-1-1 systems, the encryption algorithm SHALL be AES 256.

Mobile computing devices containing Sensitive Data (Most Sensitive Information) SHOULD **NOT** be taken outside the NG9-1-1 Entity controlled space, but if there is an overriding business need to do so then:

- Approval SHALL be documented in writing.
- Exceptions to the policy SHALL be documented in writing.
- Whenever systems containing sensitive information require repair, the repair SHALL use only authorized technicians, approved repair processes, the work done at an approved location, and the system secured in accordance with applicable non-disclosure agreements, laws, regulations, and policies to ensure that information contained on the devices is safeguarded.

4.2.2.7 Safeguarding Sensitive Electronic Information in the Cloud

Where Sensitive (Internal Use Only), Sensitive (Restricted), and Sensitive (Most Sensitive Information) data (such as private keys, credentials, passwords, certificates) is stored in the cloud it:

- SHALL use cloud vendor provided mechanisms such as Private Key protection and management methods (Key Vaults, Key Management Systems, etc.). For very high assurance security cases, NG9-1-1 entities SHOULD protect Private Keys with Hardware Security Modules (HSM).

The cloud vendor provided mechanisms used by NG9-1-1 entities:

- SHALL support audit logging, monitoring, access control and data encryption when Services are offered as Software as a Service model (SaaS).
- SHOULD adhere to broadly accepted security conventions, e.g., NIST-800, CIS Controls, or other locally applicable controls.

If a NG9-1-1 entity requires more customization capabilities, especially when operating in multi-cloud or hybrid environments, it may select a non-cloud vendor provided that the service supports at least the same level of security features provided by cloud vendors.

Note that usually 3rd party solutions, especially based on open-source, require more configuration, cloud integration effort, management for deployment and scaling than cloud native solutions but often provide greater flexibility, more advanced features or wider range of authentication methods.

Cloud data protection is critical for any NG9-1-1 Entity which utilizes the cloud. The cloud vendor must have strong internal controls in place and meet compliance standards. The vendor also must offer SLA (Service Level Agreement) which guarantees the cloud environment is properly protected.

4.2.3 Transport and Shipping of Electronic Media and Devices

- Media or devices containing Sensitive (Most Sensitive Information) SHALL be hand delivered by the Data 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.

4.2.4 Safeguarding Printed Information/Material

4.2.4.1 Sensitive (Internal Use Only) – Printed Material

- Inside Controlled Space user(s) SHALL:

  - Ensure Printed Material is kept away from visitors who have no need to see the information.
  - Observe sending and receiving fax machines with authorized personnel or use fax machines in offices/areas where access is limited to authorized personnel.
  - Ensure that Printed Material is shredded when no longer needed.

- Outside Controlled Space user(s) SHALL:
  - Ensure Printed Material is secured from unauthorized access.
  - Ensure Printed Material is kept in the direct supervision of the custodian.
  - Ensure Printed Material is in direct supervision of the Data Custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).
  - Observe the printer or copier with an authorized person for the information.
  - 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.
  - Supervise fax machines that are located outside the controlled space with authorized personnel.
  - Ensure Printed Material is shredded when no longer needed.

4.2.4.2 Sensitive (Restricted) – Printed Material

- Inside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from casual observers.
  - Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe). However, if the controlled space is only accessible to authorized individuals, it is not necessary to keep hidden or physically secured when unattended.
  - Monitor the printer or copier unless printer/copier is in an office/area where access is limited to authorized personnel.
  - Ensure Printed Material is hand delivered by originator or Data Custodian.
  - Use double envelopes with the inner envelope marked "Private" when using internal mail.
  - Supervise sending and receiving fax machines with authorized personnel or use fax machines in offices/areas where access is limited to authorized personnel.
  - Ensure Printed Material is shredded when no longer needed.

- Outside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from casual observers.
  - Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).

- Ensure Printed Material is in direct supervision of the Data Custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).
- Monitor the printer or copier with a person authorized for the information.
- 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.
- Monitor fax machines that are located outside NG9-1-1 Entity controlled space with authorized personnel.
- Ensure Printed Material is shredded when no longer needed.

4.2.4.3 Sensitive (Most Sensitive Information) – Printed Material

- Inside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from casual observers.
  - Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe).
  - Monitor the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.
  - Ensure Printed Material is hand delivered by the originator or Data Custodian.
  - Ensure Printed Material is not faxed.
  - Ensure Printed Material is shredded when no longer needed.
- Outside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is never taken outside the controlled space.
  - **However, if there is an overriding business need to take Printed Material outside the controlled space, then:**
    - Obtain approval from a Senior Manager.
    - Kept away from casual observers.
    - Kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
    - Stay in direct supervision of the custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).
    - Monitor any print/copy outside the controlled space.
    - Hand delivered by the data owner or data custodian.
    - Not be faxed.
    - Ensure Printed Material is shredded when no longer needed.

4.2.5 Disclosure of Information

Some data maintained by a NG9-1-1 Entity may be placed in the public domain and publicly discoverable or be subject to a public records request. In 9-1-1, it is typical to receive public records requests for 9-1-1 call records. The communications, information,

and data in any form that is associated with a session between a 9-1-1 caller and a PSAP is sensitive.

- The Data Protection Policy SHALL define what data can be placed in the public domain and what data is exempt from public disclosure.
- The Data Protection Policy SHALL define who may request what types of data and how those requests are to be made. A possible example of this would be limiting 9-1-1 call records to the individual making the call, law enforcement, and/or court orders. Refer to local laws and regulations for further guidance.
- Documentation for public records requests SHALL be maintained in accordance with the 9-1-1 Entities retention requirements. These documents will contain, at a minimum, who requested the data, when it was provided, and what was provided.

4.3 Risk Management

Risk Management is a process that helps Entities make better informed decisions on how to handle potential risks. This process assesses the likelihood of vulnerabilities being exploited by a threat source and pairs that with mitigating controls and risk tolerance. Risk Management is not something that is done just once, it is a continual process that needs to be re-evaluated as vulnerabilities and threats evolve or when changes to a NG9-1-1 system are made. Vulnerability, threat, and risk are defined as follows:

Vulnerability - a weakness that can be exploited. Alternatively, a weakness in system security procedures, design, implementation, internal controls, etc. that could be exploited to violate a security policy.

Threat - anything or anyone that can exploit a vulnerability. Alternatively, any circumstance or event with the potential to cause harm by adversely affecting the confidentiality, integrity, and/or availability of a resource.

Risk - the likelihood and cost of a particular event occurring. Alternatively, the probability that a particular threat will exploit a particular vulnerability of a system.

All this points to the fact that modern cybersecurity protection, as mentioned, is an exercise in risk management. The task of risk management must balance the identification of threats, assessment, eradication, and where possible, vulnerabilities and available resources.

A risk management process may follow these common steps:

1. Identify the Assets to be protected
2. Identify existing and possible future threats
3. Asses existing and possible future vulnerabilities
4. Assess risks
5. Mitigate risks

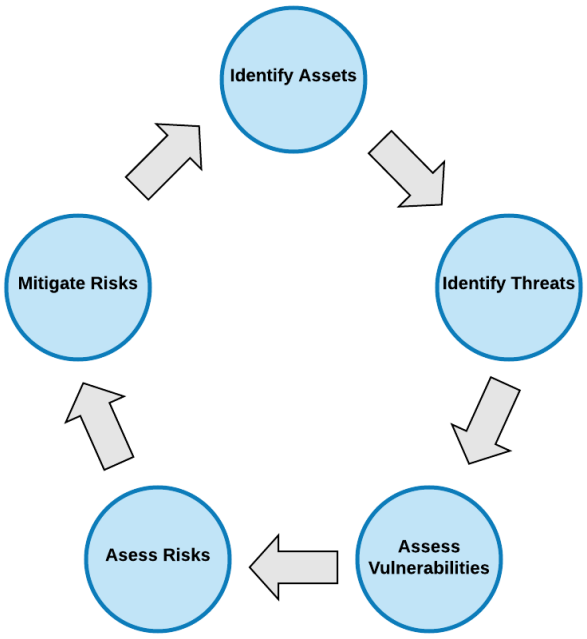

Figure 4-1 Risk Management Cycle

In November 2019, the Cybersecurity & Infrastructure Security Agency produced the *Cyber Risks to Next Generation 9-1-1* [12] publication. A chart from that publication outlining common threats to an NG9-1-1 system is shown below in Figure 4-2 Potential Risks to NG9-1-1 Systems. At a minimum, these threats should be addressed through the Entity's risk management program. Additional threats will vary and will need to be assessed.

User and Devices	Network Infrastructure and Connections	Data, Applications and Services
• **Data breaches**: Data on device is accessed, manipulated, or stolen • **Insider threats**: Employees or other authorized personnel steal, corrupt, or destroy data • **Malware**: Download of malicious software (e.g., botnets, viruses, spyware, Trojans, rootkits) • **Ransomware**: Use of software to block computer systems for the purpose of extorting a ransom • **Spear-phishing**: Targeted social engineering attacks enable criminals to access sensitive data • **Spoofing**: Unauthorized device masquerades as an authorized device	• **Denial-of-service attack**: Attackers overload network resources with requests for access, straining the operability and capacity of the network; or use RF Jamming techniques to prevent wireless, cellular, broadband, or land mobile radio (LMR) communications. • **Man-in-the-middle attack**: Wireless link between the user device and the tower may be susceptible and allow attackers to steal data or monitor conversations • **Telephony-Denial-of-service-attack**: Use of Voice over Internet Protocol systems to overwhelm the PSAP's phone system, rendering the center incapable of placing or receiving calls • **Unauthorized network access**: Bypass of authorized methods and procedures	• **Malicious applications**: Attackers create apps that appear to be safe but allow them to steal, corrupt, or modify data, eavesdrop on conversations, or acquire data on the location of victims and/or first responders • **Swatting**: Manipulation of IP-based 911 calls to indicate the call is originating from a location at which a most serious criminal act has taken or is taking place, prompting local PSAP to dispatch a Special Weapons and Tactics (SWAT) team to the address • **Unauthorized data access**: Attackers can access sensitive databases (e.g., law enforcement, health records) to steal, modify, or corrupt the data
Consequences: Any of the risks above can impact communications and operations in a negative manner and disrupt: • Confidentiality—*Ensures that data is only accessed by those authorized to see it;* • Integrity—*Ensures that data is trustworthy and is not altered through transmittal, storage, or retrieval, and/or;* • Availability—*Ensures that the infrastructure is operational and committable to its intended purpose.*		

Figure 4-2 Potential Risks to NG9-1-1 Systems

Most risks that a PSAP or their NG9-1-1 Authority has may not be directly controlled by that entity; they may be controlled by a contractor or subcontractor to that agency. The agency may require its contactors and their subcontractors to maintain risk registers, but the agency cannot properly evaluate or be held accountable for such risks.

- A NG9-1-1 Entity SHALL have a documented Risk Management process that, at a minimum, evaluates vulnerabilities, threats, and risks.
- A NG9-1-1 Entity SHALL have a documented risk acceptance form.
- There SHALL be a risk acceptance form covering every identified risk the entity has direct control over.
- Each risk acceptance form SHALL be signed off by a senior level manager within a NG9-1-1 Entity with the authority to accept the risk on behalf of a NG9-1-1 Entity.
- A NG9-1-1 Entity SHALL annually, at a minimum, reassess all risk management forms. Critical and high-level risks SHOULD be reviewed and reassessed at least monthly.

Risk can be addressed in four ways. An Entity may use a single way or a combination of ways. The four ways are risk reduction, avoidance, transfer, and acceptance. These are defined below.

1. Risk Reduction

Risk reduction involves implementing one or more mitigating security controls to reduce or eliminate the likelihood of the risk.

This is best for activities where risk can be reduced or eliminated through available resources.

2. Risk Avoidance

Risk avoidance involves stopping the function or activity that is threatened by the risk.

This is best if the likelihood of a risk exceeds the risk tolerance (unwilling to accept the risk) of the Entity and risk reduction exceeds available resources or is not an option. This is not always possible as there may be situations where a function or activity must be performed. If this exceeds the risk tolerance of the Entity and the function or activity must be performed, then risk reduction, acceptance, and/or transfer must occur.

3. Risk Acceptance

Risk acceptance occurs when a NG9-1-1 entity acknowledges and accepts a risk. This risk may be a result of technological limitations that prevent compliance, or it may be a risk that is deemed cost prohibitive to fully eliminate. Risk acceptance is a documented process that is acknowledged and accepted by authorized individuals. Each risk acceptance form should be signed by an executive or senior level manager with authority to accept the risk on behalf of a NG9-1-1 Entity. If risk acceptance is part of, or in relation to, a contract, it is highly advisable to consult with legal counsel.

A risk acceptance form should quantify the vulnerability, threat, likelihood, and impact to a NG9-1-1 Entity. For cybersecurity risk acceptance, this is commonly accomplished using qualitative assessment. Qualitative assessments use a scale like very low, low, moderate, high, and very high or a numeric range like 1 to 10 or 1 to 100. Qualitative is used because there is usually not enough data to perform a quantitative assessment.

For more information on risk acceptance or ideas on how to build a risk acceptance form, please review NIST 800-30 Rev 1, *Guide for Conducting Risk Assessments* [13].

4. Risk Transfer

Risk transfer involves transferring a portion of the risk to another Entity. This generally involves purchasing insurance or entering into a contract with a third party. PSAPs and other 9-1-1 Authorities are usually unable to transfer risk, except

through special insurance arrangements. Remember that this does not transfer responsibility. The Entity is still ultimately responsible for the activity or function. However, with risk transfer, the Entity shifts some of the financial burden associated with the risk.

This is best suited for situations where the likelihood of a risk is lower, and the financial impact of the risk is high. The cost to transfer the risk increases the higher the likelihood of a risk and/or the greater the financial burden shifted.

A senior level manager with responsibility and authority for an NG9-1-1 system is required to accept all identified risk and this responsibility cannot be delegated. Many senior managers could hold authority for different areas of a NG9-1-1 system with some responsible for multiple areas. A senior level manager accepting risk should also hold financial and legal responsibility for that area of a NG9-1-1 system.

4.3.1 Threat Vectors

A threat vector is a means by which malicious actor could gain access. Some common potential threat vectors are ingress points, egress points, and demarcation points. Mitigating threat vectors is a top priority for an effective security posture. This entails mitigating physical and electronic access to ports, devices, cables, and/or components.

- The PSAP and authority having jurisdiction SHALL ensure that Service Level Agreement(s) (SLA) addresses all threat vectors.

Some common threat vectors include (but are not limited to) the following:

- Network
- User
- Email
- Web Application
- Remote Access
- Mobile

Threat vectors are often directly tied to common cybersecurity attacks such as:

- Malware
- Phishing
- Denial of Service (DoS)
- Session Hijacking
- Credential Reuse
- Brute Force

Understanding the threat vectors of the NG9-1-1 network will help in establishing effective security measures capable of avoiding threats.

4.3.2 Threat Protection and Mitigation

The Communications Security, Reliability, and Interoperability Council (CSRIC) VII submitted to the FCC a report titled *Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations* [14], which was released by the FCC on September 16, 2020. This document contains informative advice regarding mitigation strategies for various types of cyberattacks. Those techniques are largely based on the National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) [15]. The NIST CSF provides a recognized and widely adopted approach to cybersecurity defense.

This CSRIC report [14] strives to reinforce existing valid cybersecurity risk management strategies, best practices, and recommendations. It goes on to explain the concept of the threat landscape specific to emergency communications. In addition, this CSRIC report provides updated recommendations for mitigating threats and includes updates to recommendations from previous CSRIC Best Practices work.

CSRIC VII also submitted to the FCC a subsequent report titled *Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and Next Generation 9-1-1 (NG9-1-1) Networks* [16], which was released by the FCC on March 10, 2021. This report was based off the Council member's experience, available literature, and documented industry experience. It identifies the potential cost and level of effort for security measures, providing a roadmap for organizations of different sizes and capabilities in ways to improve their cybersecurity posture.

Together, these CSRIC VII reports contain a wealth of informative material on cybersecurity-related subjects, including threat protection, mitigation techniques, strategies, and best practices. They provide examples of mitigation techniques that can lessen the impact of cyberattacks typically seen in the Public Safety realm. These mitigation strategies are essential to a well-designed cybersecurity defensive strategy.

The following are excerpts from the CSRIC reports [14][16] and the NIST CSF [15].

4.3.2.1 9-1-1 Attack Surfaces

Attack *surfaces* are defined in terms of *attack vectors*. An attack vector is any avenue that a bad actor can use to exploit systems, networks, and information. An *attack surface* is the sum of all the *attack vectors* that exist for an organization (i.e., the total surface area of potential system exposure, including systems in the data center, laptops in the field, cloud applications, connected industrial systems, or any combination of these hybrid environments that organizations may have). NG-911 systems have the same attack surfaces as other public and private sector IP networks.

4.3.2.2 Attack Surface Descriptions

Within an NG9-1-1 context, there are seven (7) attack surfaces associated with the emerging NG9-1-1 system. Figure 4-3 The Seven NG9-1-1 Cyber Attack Surfaces illustrates these attack surfaces.

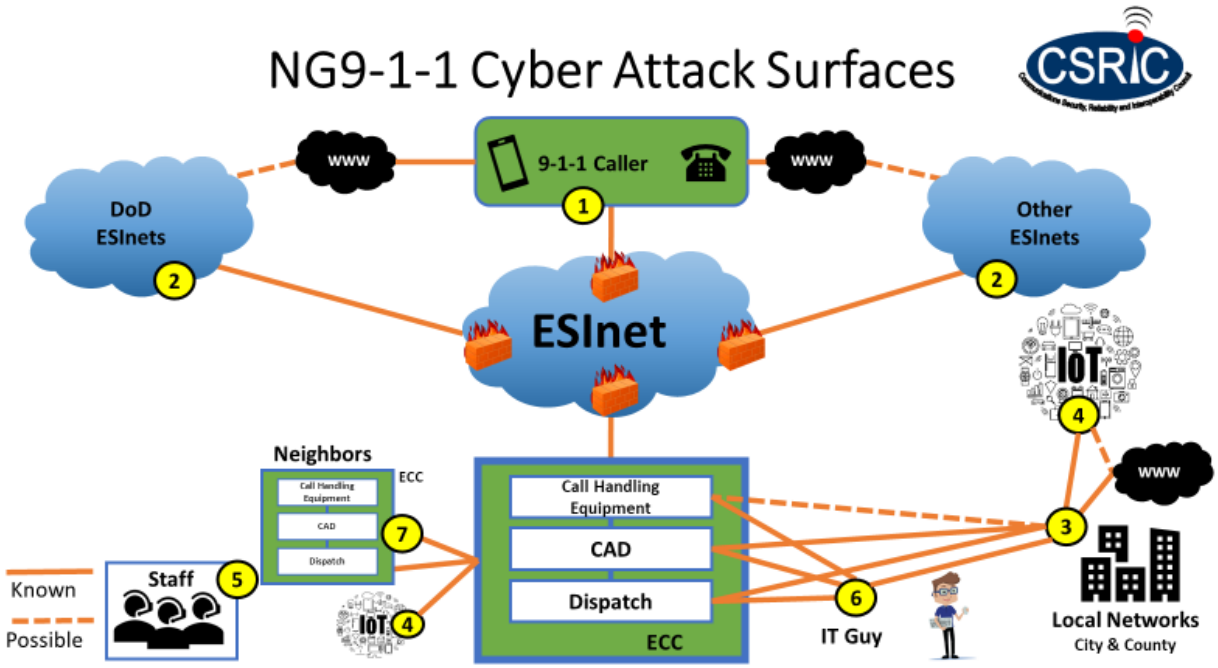

Figure 4-3 The Seven NG9-1-1 Cyber Attack Surfaces

- Attack Surface #1: 9-1-1 Caller (origination networks – voice, text, pictures, video, data)
- Attack Surface #2: Other connected ESInets
- Attack Surface #3: Local network connections (WWW, admin, support, Gov't)
- Attack Surface #4: Internet of Things (local, on-site, remote management)
- Attack Surface #5: Staff (on-site, admin, CPE, CAD, remote access)
- Attack Surface #6: IT support (on-site, remote management)
- Attack Surface #7: Other connected jurisdictions (within ESInet, backup sites)

See the CSRIC *Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations* [14] for a detailed description of each of the above-mentioned attack surface descriptions.

4.3.2.3 The NIST Cybersecurity Framework (CSF)

The NIST CSF [15] is a voluntary framework developed by NIST working with various stakeholders to identify existing standards, guidelines, and practices that could be integrated into a guiding framework for reducing cybersecurity risks to critical

infrastructure. The framework core describes a set of activities that can be used to achieve a desired cybersecurity-specific outcome. Following the NIST CSF model can help identify where specific threats might fit and how to mitigate those threats.

4.3.2.4 Examples of Mitigation Techniques

The single most fundamental solution to mitigate cyberattacks is to perform continuous cyber monitoring. As a best practice, a comprehensive continuous monitoring program is utilized to assess changes that could have impact to an established Security Posture in NG9-1-1 systems. Performing other cyber tasks, as described below, is also important to help to ensure a well-rounded risk management program.

In addition to continuous monitoring, these are additional steps that can be taken to help mitigate the impacts from cyberattacks.

- Perform vulnerability assessments to identify weaknesses, threats and/or risks to the system. Vulnerability assessment tools should be used at a minimum of every 90 days across the entire infrastructure.
- Utilized the 3-2-1 backup strategy [17]. This entails having three (3) backups on two (2) different forms of media storage (such as cloud, tape, external drive, flash drive) that can be connected on demand.
- Have a written cybersecurity response plan in place and test it at least quarterly.
- Ensure you have valid backups and test those backups at least quarterly to ensure you can recover from your backups.
- Have cybersecurity insurance but only use it to pay for third-party assistance to aid with recovery. DO NOT use it to pay ransom.
- Get the best firewall you can afford.
- Use network segmentation and place sensitive info behind additional firewalls and protective measures.
- Follow least privilege by limiting user privileges to only what is needed to accomplish each specific job's duties.

There are two types of vulnerability assessment scans, external and internal. External scans analyze public facing IP addresses, while internal scans analyze the entire network from inside. CSRIC VII recommends weekly scans of externally visible network connections. NENA also recommends weekly internal scans. If the implemented cybersecurity monitoring solution provides weekly reports and regular external analysis, then additional vulnerability assessments could instead be done annually. Assessment tools should be updated as frequently as possible, but not less than once a week.[3]

[3] See the "Findings" section of the CSRIC *Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and Next Generation (NG9-1-1) Networks* [16] for greater detail of these steps.

4.4 Change Management

Change management is a formalized and structured process that manages and evaluates the impact of change to a NG9-1-1 environment. It is used to evaluate the impact of a change and mitigate potential issues that may arise. Change management also helps ensure that affected staff are aware of, and trained in, changes that affect them.

There are three types of changes defined for a NG9-1-1 Entity:

1. **Routine Changes:** Routine changes are repetitive low risk changes that have been authorized for implementation without the need to go through a full change management process every time. An example of a common routine change is the creation or deletion of a user account.
2. **Planned Changes:** Planned changes are known of in advance, offering the time to fully evaluate and address the impacts. An example of a planned change is the installation of a new CAD system.
3. **Unplanned Changes:** Unplanned changes are changes that must be made without sufficient time to fully evaluate the impacts. This change will follow a different process, may have a different approval requirement, and may not be documented until after the change has been implemented. An example of an unplanned change is replacing a critical server that is no longer operational.

- All changes to equipment and/or configuration of a NG9-1-1 system SHALL be reviewed and approved in accordance with the Change Management policy.
- All changes to equipment and/or configuration of a NG9-1-1 system SHALL include a documented security review.
- All changes SHALL be documented. This may consist of new documentation for new equipment or updates to existing documents for configuration changes.

Note: For unplanned changes, any of the SHALL statements above may need to be completed after the change.

Changes should be reviewed and approved by a change control board. A change control board will typically consist of members representing different aspects of an Entity. Subject matter experts should be utilized on the change control board and/or during the change management process.

5 Operations Management Domain

The Operations Management Domain for NG-SEC helps ensure that a NG9-1-1 system continues to operate securely. It addresses security training, monitors, and assesses the current state of the system and covers what to do if there is an issue.

5.1 Cybersecurity Training

5.1.1 Cybersecurity Awareness Training

It is the responsibility of everyone in a NG9-1-1 Entity to be vigilant for any suspicious or unusual activity. Often the detection of a cybersecurity incident results from a staff member noticing abnormal or suspicious behavior. The best way to train individuals on how to recognize and report suspicious activity is through Cybersecurity Awareness Training. Cybersecurity Awareness Training entails the education of all users, including third-party users, who may access any part of a NG9-1-1 system. This training needs to highlight identified potential risks and threats that a user may encounter. NENA recognizes that Security Awareness Training is critical to any organization's security strategy and security operations.

- All users of a NG9-1-1 system SHALL be trained 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 users of a NG9-1-1 system SHALL, at a minimum, complete Cybersecurity Awareness Training annually. This training will include instruction on how to recognize potential threats that a user could reasonably expect to encounter. Cybersecurity Awareness Training must also use parts of the Cybersecurity Incident Response Plan, which includes the notification and escalation process for users, the primary points of contact, and the process for submitting a cybersecurity event.

5.1.2 Technician Security Training

There are two ways commonly used to pre-assess a technician's skill and knowledge in a technological area: certifications and experience. A certification is much like an educational degree or diploma. It signifies a base level of knowledge in all areas covered by the certificate, degree, or diploma. Often an individual will have greater knowledge in some areas and a base level in others. Whereas experience on the other hand is gained over time by working in a specific area or areas.

Certifications are provided by many professional organizations for specific technological areas. These are usually the easiest to assess as a technician will have a currently valid certificate or they will not. Certifications may indicate the completion of a training program, signify entry level knowledge, or indicate advanced knowledge. They can be for a specific application or program or can indicate knowledge in a specific area like network architect or firewalls. Most technician certificates require an individual to demonstrate a specified level of knowledge, often through a testing process, and sometimes require a minimum level of experience. To maintain some certifications, an individual may be required to annually complete continuing education credits within the field to maintain the certification.

Common technician certifications that may be seen in a NG9-1-1 environment include the following:

- CompTIA – SEC+
- CompTIA – CASP+
- Certified Ethical Hacker (CEH)
- Certified Information Systems Security Professional (CISSP)
- Certified Authorization Professional (CAP)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Cisco – CCNA (Cisco Certified Network Associate)
- Cisco – CCNP (Cisco Certified Network Professional)

This is just a small example of the relevant certifications available. When looking at certifications, focus should be on those that best meet the requirements of the position and equipment being maintained.

The other way is experience. Experience is gained over time by working in the field with different networks and software components. Experience is harder to assess than certifications, but it is no less important. Often a technician with experience with a specific device, application, or program can perform the necessary actions on that item better than an individual with just a certificate.

It is vital that technicians working on a NG9-1-1 device, program, or application have a sufficient level of knowledge for what they are tasked to do. For example, a technician that is experienced in Active Directory may not have the knowledge to setup and configure a firewall or vice versa. Many skill sets are focused on a specific area. This does not mean that a technician cannot have experience and/or training in multiple areas. The important part is that the technician has a sufficient combination of knowledge and skill to perform the tasks required.

- Entities responsible for system and/or security administration (including those contracted to do such tasks) SHALL employ individuals who have received current security training in their assigned area of responsibility. Security operations, administration, and maintenance training applies to any individual responsible for securing and/or working on any part of a NG9-1-1 system. A NG9-1-1 Entity can require a service provider to supply validation and assurances of a technician's knowledge and skill to perform a task.

5.2 Security Assessments

A security assessment is done to identify potential weaknesses in a NG9-1-1 system. Typically, these will identify missing patches, misconfigurations, open ports, etc. They are normally arranged in order of criticality. When determining the criticality/risk, consideration is given to both the potential for the risk to result in a successful attack and the potential

level of negative impact if it succeeds. The higher the criticality, the higher the risk. All identified findings need to be addressed with a focus on findings with a higher criticality before those with a lesser criticality. To aid in that decision making, a classification system may be helpful. For example, the classifications could be as shown below in Table 5-1 Classification.

Table 5-1 Classification

Classification	Description
High	Expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Medium	Expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	Expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

There may be times when a finding cannot be corrected. These still need to be addressed. This can be done through mitigation, to the extent possible, to reduce the impact of an accepted risk. The remaining risk must be accepted. Acceptance needs to be signed off by a senior manager authorized to accept risk for that respective area on behalf of a NG9-1-1 Entity.

Security assessments can be conducted internally and externally. Internal assessments are used to "self-check" an Entity's compliance with security standards and/or policies. An external audit leverages a non-biased third party to independently perform the audit. Both methods are valid and useful. Security assessments should use various methods to assess the security of networks, processes, applications, services, and platforms including automated tools, checklists, documentation review, penetration testing, and interviews.

- A security assessment SHALL be conducted, at a minimum, annually. This may be an internal or external assessment.
- An external assessment SHALL be done, at a minimum, once every 3 years. This SHOULD be done by a different firm/organization than was used previously.
- An external assessment, to include gap analysis, SHALL be documented and provided to a NG9-1-1 Security Manager or their designated representative.
- All findings from a security assessment SHALL be addressed. If unable to address the finding fully, a NG9-1-1 Entity must accept any residual risk.
- Security assessments SHALL be retained for a minimum of five years and in accordance with local retention policies. If all parts of an audit no longer cover any area of the current NG9-1-1 system, it may be disposed of earlier if allowed by local retention policies.

5.3 Availability

Availability means that data is accessible to authorized individuals when needed. Critical systems need to be highly available. Availability provides a means of assuring that all systems and services have a level of uninterrupted access and/or use under normal conditions. There are numerous things that affect availability. These include, but are not limited to, device failure, errors, environmental issues (heat, static, flooding, power loss, etc.), and cybersecurity incidents.

Availability is expressed as a percentage of time that a resource can be used for its intended purpose and is typically referred to as nines of availability. The higher the nines the more it costs. This cost reflects the expense needed to build in the redundancy and resiliency needed for the level of nines desired. Table 5-2 Availability below, lists some commonly found levels of nines and the maximum down time allowed annually for that level of nines. This down time is cumulative over the year and may happen all at once or be spread out over different intervals throughout the year.

Table 5-2 Availability

Availability	Approximate downtime
90% (1-nine)	36.5 days/year
99% (2-nines)	3.65 days/year
99.9% (3-nines)	8.76 hours/year
99.99% (4-nines)	52 minutes/year
99.999% (5-nines)	5 minutes/year
99.9999% (6-nines)	31 seconds/year

Critical and non-critical services may have different availability levels. Some services may be unavailable while others may still be available but with degraded functionality. For example, if call data linked to CAD is not available; a manual lookup can provide the same results though it is a slower process. In this case the service is still available. Now if the call data server is not available, then the service is not available and would be down.

Availability comes into play during NG9-1-1 system design and with Service Level Agreements (SLA) /Service Level Objectives (SLO) for contracted portions of a NG9-1-1 system. Remember, the greater the desired availability, the higher the cost. With higher availability there is often greater redundancy. Redundancy is essential for maintaining availability. With a redundant service you can have one side down while the other is still providing the service and maintaining availability.

When using SLAs, there should be a remedy when the vendor fails to maintain the specified availability by exceeding the allowable down time. System availability during a

maintenance window is subject to the terms and conditions of the SLA and is often excluded from the allowable downtime.

Some of the building blocks used to help create a highly available network include, but are not limited to, the following:

- Redundant and physically diverse paths consisting of LAN switches, servers, routers, WAN links, premise wiring, HVAC (Heating, Ventilation, and Air Conditioning), etc.
- Geographically diverse and redundant NG9-1-1 entity functions
- Fail over of critical functions (Active / Active, Active / Passive)
- Teamed[4] NICs (Network Interface Card) in servers and mission-critical desktop computers
- High availability or redundant firewalls
- Out-of-band communication links
- RAID arrays (Redundant Array of Independent Disks)
- High Availability server designs
- Backup power supplies, generator, and UPS systems
- Performance monitoring tools and resources
- Secure facilities environment
- Mutual aid agreements

The goals for ensuring a highly available network are as follows:

- Identify and document all single points of failure and their alternative strategies. If one of the high availability elements is down, the status should be made known to a NG9-1-1 Entity and the management entities.
- Develop, document, and test a plan to achieve High Availability. Testing of those plans should be done at least annually, with the results documented. Any identified issues should be addressed.
- Perform annual drills and produce action plans to address any observed issues.
- Plan for diverse down-time windows to minimize business impact.

5.4 Inventory

Having an accurate and up to date inventory of all devices, software, and data is an essential foundation for security. Knowing what you have, and its importance, helps determine what protections are needed. It also helps in being able to determine what version/patch level software and firmware are at, and more easily identifying what should not be there. Inventories can be done manually, using a device, using an application/program, or a combination of these. An automated process using a device and/or application/program is highly recommended as this will provide a more up-to-date

[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.

inventory and help to more rapidly identify unauthorized hardware, software, and applications.

It is also important to inventory software libraries. A software library in this context refers to a collection of preconfigured modules or routines that can be used by different programs. In Windows, a common example of this is a Dynamic-Link Library (DLL). Software libraries are harder to control as some software libraries are included with installations like Java and some programs are written to work with specific versions. A program may specify the use of a compromised software library and when the program attempts to use it and does not find it, it may attempt to reinstall it.

The ability for full inventory may be limited by vendor span of control and contract.

An inventory SHALL, at a minimum, document and track the following:

- Devices
  - Device name
  - Identification (make, model, and serial number)
  - End of life date
  - Firmware version(s) (a device may have multiple components with firmware)
  - Primary location
  - Primary owner/responsible party
  - Highest classification level of data used on/by device
  - Contract/warranty
- Software and applications
  - Software/application name
  - Software/application version
  - Number of licenses
  - End of life date
  - Device(s) installed on
  - Highest classification level of data used on/by software/application
  - Contract/warranty
- Data (by group)
  - Classification level
  - Storage location
  - Data Owner
  - Data Custodian
- Cloud/third-party services
  - Provider
  - Contact info
  - Service provided (i.e., data storage, CPE, e-mail, connectivity)
  - Contract end date
  - Entity administrator/point of contact
  - Highest classification level of data on or used by service

    - Contract/warranty
- Software libraries
    - Path
    - Manufacturer
    - Version number

As a best practice the inventory should be used to establish a critical impact analysis if a particular asset is threatened. This can align with a Business Continuity plan to contain, minimize, and isolate a threat to security.

An inventory will assist in determining where trusted and untrusted zones exist. The type of zone may alter the security platform, network configuration, and design for each ingress and egress access point whether hardware or software provided.

5.5 Patching and Updating

Patches are applied to hardware and software to either add new functionality or to correct a vulnerability or update a capability. Firmware, BIOS (Basic Input Output System), drivers, operating systems, software, and/or applications typically have periodic patches and updates. Updates to add new functionality generally follow a planned release cycle and are known of well in advance. Vulnerability fixes on the other hand follow a much shorter timeline. Vulnerabilities are found over time and once discovered are often rapidly exploited. The Common Vulnerability Scoring System (CVSS) [18] is an industry standard for ranking vulnerabilities. They are ranked from 0.0 (low) to 10.0 (critical). As vendors and security organizations become aware of vulnerabilities, they should issue either alerts or advisories for the vulnerability. These notifications should include the severity of the vulnerability, a description of what the vulnerability exploits, indicators that the vulnerability has been exploited, and provide permanent and/or temporary fixes to mitigate the vulnerability. Permanent fixes are preferred over temporary fixes. Which to use will depend on the situation. If a NG9-1-1 Entity has been made aware of a vulnerability, it should check for indicators of compromise throughout a NG9-1-1 system.

Note that timely patching is also an effective protection against Brute Force attacks.

- A NG9-1-1 Entity SHALL validate all necessary patches are installed at least monthly.
- Once a mitigation control or patch has been approved through the change management process, and has undergone appropriate testing, it SHALL be applied as soon as possible.
- After a patch or mitigation control is applied to fix a vulnerability, a NG9-1-1 Entity SHALL verify that there is no evidence that the vulnerability was exploited in a NG9-1-1 system.
- A NG9-1-1 Entity SHALL establish timelines for patching CVSSs based on criticality. It is recommended that critical CVSS be patched within 48 hours or less of disclosure.

For more information, please see NIST SP 800-40, *Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology* [19].

5.6 Continuous Monitoring

Continuous monitoring is an important tool in maintaining the security of a NG9-1-1 system. It provides information on the state of the system and can be used to detect anomalies, track down root causes, and aid in incident response. It provides insight into the system.

5.6.1 Time Synchronization's Relationship to Continuous Monitoring

Time synchronization is important for event correlation. Time synchronization is used in managing, troubleshooting, and securing systems as well as for other network functions like authentication and continuous monitoring.

- Time synchronization SHALL be in accordance with the Time Server specifications in NENA-STA-010.3 [6].

5.6.2 Security Event Logging

Security event logging (as distinguished from NG9-1-1 call logging as defined by NENA STA-010) is important in detecting and tracing cybersecurity incidents. Many applications and devices can provide logging. Logging helps provide early indications that something is going on and can help determine how far an incident has spread. What can be detected depends on what is being logged. It is important to log only what is necessary so that the process of logging does not consume too many resources and slow down systems. The more relevant the logs in relation to an incident, the better it can be detected/tracked. Many malicious attacks attempt to disguise their actives as normal network traffic so you will need to understand what normal looks like for your environment.

Security Event Logging should be centralized and standardized. However, NG9-1-1 "Security Event Logging" has not yet been defined within the NG9-1-1 Logging Service. These Log Events will be specified in a future NENA document.

Each NG9-1-1 Entity SHALL:

- Have all logging applications and device clocks synchronized with the time server specified in Section 5.6.1 Time Synchronization's Relationship to Continuous Monitoring. This allows logs to be easily correlated between different devices and applications through their timestamps.
- Have sufficient logging to be able to trace and correlate events throughout a NG9-1-1 Entities' system. This may require additional logging requirements for administrative accounts. See note below.

- Review logs at least weekly by an individual. This should be done more frequently with the ideal being as close to real time as possible. To achieve this, automation will be required. The NG9-1-1 Logging Service includes standardized log retrieval functions that can assist such automation. See Section 5.6.3 Information and Event Management.
- Protect logs from unauthorized deletion or modification.
- Retain logs in accordance with local retention requirements.

For more on log management please refer to NIST SP 800-92*, Guide to Computer Security Log Management* [20].

5.6.3 Information and Event Management

Event management looks at log files as well as other security events from various devices on the network. Currently there are three primary areas associated with this. Security Event Management (SEM), Security Information Management (SIM), and System Information and Event Management (SIEM).

A SEM monitors real-time information by looking at log files and other security data and flags the most important data. A SEM generates automated alerts based on specified thresholds and may also perform other automated actions depending on how it is set up. A SEM generates security dashboard content.

A SIM focuses on collection and long-term storage of log files and other security data. SIMs focus on storing data long term for later analyses. Some SIMs may filter and normalize data before passing it along.

A SIEM combines the functionality of a SEM and a SIM. A SIEM analyzes real-time and historical security data. A SIEM may also be used to demonstrate compliance and monitor resource utilization across the network.

Information and Event Management utilizing a SIEM configuration is highly recommended. This may be done internally or implemented through a third party.

5.6.4 Intrusion Monitoring and Detection

Intrusion monitoring and detection involves looking for known threats or suspicious behavior. Signature based detection is used when looking for known threats. Anomaly based detection is used when looking for suspicious behavior. These types of detection are typically handled by an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS).

An IDS is either a hardware device or software application that uses known intrusion signatures and/or behavior-based algorithms to detect and analyze traffic. An IDS sends out alerts based on defined thresholds.

An IPS performs the same services as an IDS and can also perform automated actions in response. IPS solutions should be avoided on network segments containing 9-1-1 call and call related services because it could block legitimate caller media and data. If it is decided to implement an IPS solution, careful consideration should be used when selecting, configuring, and implementing IPS solutions on a 9-1-1 call handling network segment.

An IDS or IPS can be placed on a wired network, wireless network, and/or on an endpoint. IDS's and IPS's operate of off configured thresholds, deny lists, allow lists, and/or alert settings. A threshold is a value or range above or below which an alert is triggered. Deny lists are addresses, protocols, services, programs, etc. that are blocked. Allow lists are addresses, protocols, services, programs, etc. that are allowed. Alert settings define the severity and frequency of alerts. The capabilities and limitations of each of these will vary between different IDS's and IPS's. Each of these will need to be adjusted to the environment and will dictate when an alert and/or action is taken. There will be alerts on legitimate traffic, called false positives, and things that slip through, called false negatives. No IDS/IPS will be 100%.

It is highly encouraged that IDS solutions be employed in NG9-1-1 systems. Alerts and IDS need to be monitored at least daily. Real-time monitoring would be ideal. This should be done by one or more individuals using an automated solution that can help organize, correlate, and prioritize the alerts. It is also recommended that 9-1-1 security teams take swift action on the alerts generated to prevent system interruption.

Security monitoring systems, e.g., Intrusion Detection Systems (IDS), Firewalls, Event Logs, Security Information Event Management (SIEM), etc. require periodic review.

- There SHALL be a defined process or procedure identifying when and how often the periodic review of security monitoring systems will be done.

5.6.5 Incident Detection and Response

Early detection is key to identifying and containing a security incident. There are many tools that aid in this. The most common aids for incident detection are a SIEM, IDS, and/or IPS. Staff members are another good source for identifying abnormalities or suspicious behavior. Once an incident has been detected, trained and experienced staff will be needed to triage the incident, understand its scale, and understand its potential impact to scope the type of response. This response is defined in a Cybersecurity Incident Response plan, which is a formal, written plan detailing how an organization will respond to computer security incidents. Some examples of security incidents include malware attacks, ransomware, hacking attempts, critical service outages, denials of service, and directed disruptions.

A Cybersecurity Incident Response Plan outlines an NG9-1-1 Entities response to a cybersecurity incident.

- Cybersecurity Incident Response plans do not need to be complex and should be adaptable to different situations.
- Cybersecurity Incident Response plans need to be periodically evaluated to ensure they are still viable.
- Cybersecurity Incident Response plans need to be tested, and individuals responsible for sections of the plan need to be trained in those areas.

A Cybersecurity Incident Response Plan should include the following topics:

- **Preparation:** Ensuring sufficient security measures are in place and that an NG9-1-1 Entity is ready and able to respond. This should include when and how to bring in outside help along with a list of available resources. Some of these may require purchasing authority. This outside help could be through a contracted service, a Community Emergency Response Team (CERT), or through some other entity where assistance can be obtained.
- **Detection & Analysis:** Detection is the discovery of the incident. This may be through security tools, notification by an inside or outside party, or some other method. This phase includes the declaration and initial classification of the incident.
- **Containment, Eradication, and Recovery:** It is important to contain an incident to prevent further damage. Having predefined procedures to contain an incident helps speed up the process and better ensure successful containment.
- **Post-Incident Activity:** Having a post-incident activity helps ensure that lessons learned are documented, needed improvements to security measures are made, and any needed updates to the Cybersecurity Incident Response Plan are made.

NIST 800-61 Rev 2, *Computer Security Incident Handling Guide* [21], defines these four primary areas in more detail under the "Handling an Incident" section.

- A NG9-1-1 Entity SHALL have a Cybersecurity Incident Response plan.

5.6.6 Network Operations Center (NOC) and Security Operations Center (SOC)

Security data needs to be continuously monitored, reviewed, and analyzed by skilled staff. This should be as close to real time as possible. This functionality typically resides in a NOC and a SOC. These may be internal to an NG9-1-1 Entity, or they may be outsourced. The NOC and SOC functionality may be consolidated into one entity, or each may perform some of the other's activities.

A NOC monitors the health of the network helping to make sure that it is operating within specifications. They monitor network equipment like routers, switches, and servers and other services like cloud storage, power, and environmental controls. All the components and devices that make up an NG9-1-1 system. Some NOCs only monitor activities while others may perform other IT related actions like updating, patching, or installations.

A SOC is a facility that houses an information security team. This team is responsible for monitoring and analyzing activity on networks, servers, endpoints, databases, applications, websites, and other systems. They are looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring incidents are correctly identified. They will alert the NG9-1-1 Entity, alert other specified contacts like an incident response team, and assist with the incident. The level of assistance will depend on the capabilities of the SOC.

Often a SOC alert has a classification level. An example of this is shown below in Table 5-3 Classification Levels.

Table 5-3 Classification Levels

Classification	Description / Examples
Critical*	A hack in progress, which would typically trigger the SOC to call the customer to engage them in the mitigation steps immediately.
Highly Likely*	Data traffic that indicates a hack could be imminent. That too would trigger the SOC to call the customer to engage them in the mitigation steps.
Medium	Data traffic that reveals a hack is possible but less likely to be successful due to various factors. This typically begets heightened monitoring to ensure the risk level doesn't amplify to a higher classification.
Low	Data traffic that reveals attack signatures that are not likely to succeed. Typically, the SOC would record these to assist in building attack profiles which can aid in continuous improvement of behavioral analysis techniques.

***NOTE:** In both the Critical and Highly Likely classifications, when possible, the SOC typically undertakes immediate action on their own while attempting to engage the customer. That depends on the contracted responsibilities of the SOC.

5.7 Recovery Operations

NG9-1-1 is designed to not fail, even when attacked. If the mechanisms described in the standards are implemented as described, even a severe cybersecurity incident should still result in 9-1-1 calls being answered and available responders being dispatched. It is essential that these mechanisms be implemented so that we can help individuals in need even when an attack happens. Nevertheless, we can anticipate that security incidents will happen, specific sites and systems will be affected, and recovery operations will be needed.

When recovery operations are necessary to return to normal operation, they need to follow a well thought out plan. These plans need to be developed ahead of time and tested.

There are three predominate types of plans used in recovery. There is the Business Continuity (BC) plan, the Disaster Recovery (DR) plan, and the Cybersecurity Incident Response Plan (CIRP). These plans help an Entity recover from disasters and other incidents and resume normal operations.

A BC plan is generally a more proactive approach to addressing the processes and procedures an entity or organization implements to ensure that mission-critical functions remain operative during and after a disaster. A BC plan deals with the business operations side. It involves designing and creating policies and procedures that ensure that essential business functions/processes are available during and after a disaster. A BC plan can include the replacement of staff, service availability issues, business impact analysis, and change management.

A DR plan is more reactive and outlines the steps an entity or organization takes to recover from an incident and resume normal operations. A DR plan is primarily focused on the IT side. It defines how an organization's IT department will recover from a natural or artificial disaster. The processes within this phase can include server and network restoration, copying backup data, and provisioning backup systems.

A CIRP is a reactive plan outlining the steps needed to prepare, detect, analyze, contain, eradicate, recover, and conduct post-incident activities in the event of a cybersecurity incident. The CIRP helps to minimize damage and loss during a cybersecurity incident as well as ensuring that the appropriate actions are taken.

- A NG9-1-1 Entity SHALL have the following recovery plans. They may be separate or combined. It is recommended that they are separate plans.
  - Business Continuity plan
  - Disaster Recovery plan
  - Cybersecurity Incident Response plan
- These plans SHALL be maintained offline and be accessible to recovery teams.
- These plans SHALL be tested and reviewed at least annually and updated as needed.

There are resources to help develop these plans:

- NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems* [22]
- NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide* [21]
- NIST SP 800-184, *Guide for Cybersecurity Event Recovery* [23]

5.7.1 Forensics

In the event of an incident, it is important to preserve forensic information. This information helps identify the chain of events that occurred, helps track an incident through a NG9-1-1 system, and may be used for criminal investigation and prosecution.

Forensic evidence needs to be preserved and unaltered. For legal purposes, chain of custody needs to be maintained.

- A NG9-1-1 Entity SHALL have documented procedures outlining what forensic evidence should be captured and preserved.
- A NG9-1-1 Entity SHALL have documented procedures outlining how forensic evidence should be captured.
- A NG9-1-1 Entity SHALL have documented procedures outlining how to establish and maintain chain of custody of forensic evidence in accordance with local governance.

5.7.2 System Backup and Restoration

Having backups of important information is imperative to recovering from many incidents. Backups are often essential to return to normal operations after an incident. Testing and validating the backups is fundamental to ensuring that they are effective and useful.

As part of the backup strategy, it is important to determine the following:

- **What type of information is to be backed up?** Some information to consider for backup are system images, server images, configuration files, data, data bases, log files, licensing, software, and any data or information that has a legal requirement.
- **Frequency of back up of the information.** Backup frequency determines how much data loss a NG9-1-1 Entity is willing to accept. The frequency is how often backups are done. For instance, if backups are done once a week, then the most data that could potentially be lost is the last weeks' worth. The frequency may be different for different things in a NG9-1-1 Entity. For instance, a system image may only be backed up once a year while critical data files are backed up twice a day.

5.7.2.1 Backup Strategy

A good starting point for a backup strategy is called the 3-2-1 backup strategy. With this backup strategy you have at least 3 backup copies with 2 of them stored locally on different equipment and at least 1 copy stored offsite.

A 3-2-1 backup strategy will have:

- more than one copy of the backup
- at least one backup copy stored off site
- at least one backup copy not attached to the network when not actually performing a backup

For more information on the 3-2-1 backup strategy, see *Data Backup Options* [17].

5.7.2.2 Validating and Testing Backups

It is important to validate and test backups. Validating backup checks that the backup and the data are the same. Validating backups ensures that all the required data has been backed up. Validation should be accomplished using an automated process. Often backup software includes a validation option, or an authorized third-party tool could be used. It can be done manually but is often time-consuming. Periodically testing recovery operations helps to ensure that recovery equipment and procedures continue to function as expected. Finding out that some or all the data that had been backed up is unusable during an incident will cause a lot of problems.

- A NG9-1-1 Entity SHALL have a documented backup plan.
- A NG9-1-1 Entity SHALL have documented recovery procedures.
- A NG9-1-1 Entity SHALL test their backup plan annually at a minimum.

6 Security and Risk Management Domain

6.1 Perimeter Security

While Perimeter security is important, it should not be the primary defense for any NG9-1-1 Entity. All systems must be intrinsically secure, including from an attack inside the perimeter.

- All NG9-1-1 Entity information resources SHALL be kept physically secured and protected from theft, misappropriation, misuse, unauthorized access, and damage.
- A controlled area entry and exit log SHALL be maintained for every controlled area.
- Physical access control devices/keys issued to an individual SHALL never be loaned or shared with another individual.
- A person possessing an access control device/key SHALL never use that device/key to allow access to an unauthorized individual.

The following sections were modified for NG9-1-1 from CJIS as they apply to a PSAP.

6.1.1 Physical Protections

- NG9-1-1 facilities SHALL have adequate perimeter access control. These may include fencing, video cameras, lighting, guarded access points, etc.
- The perimeter of a physically secure location SHALL be prominently posted and separated from non-secure locations by physical controls.
- All entry points to secured locations SHALL be prominently marked.

6.1.2 Physical Access Authorizations

- A NG9-1-1 Entity SHALL develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the

permanent facility officially designated as publicly accessible) or SHALL issue credentials to authorized personnel.
- Non-NG9-1-1 Entity employees who are issued any devices and/or keys that grant access to NG9-1-1 Entity facilities SHALL be sponsored by a NG9-1-1 Entity management individual.
- Documentation on sponsorship and results of all local, state, and federal guidelines (i.e., background checks) SHALL be maintained for each non-NG9-1-1 Entity employee who is granted access.
- Non-NG9-1-1 Entity employee documentation SHALL be retained for a duration defined by the local retention policy.

6.1.3 Physical Access Control

- A NG9-1-1 Entity SHALL control all physical access points (except for those areas within the facility officially designated as publicly accessible) and SHALL verify individual access authorizations before granting access.
- Everyone entering a controlled access facility SHALL follow the physical access control procedures in place for that facility.
- A controlled area entry and exit log SHALL be maintained for everyone entering and exiting a controlled area.
- Controlled area entry and exit log files SHALL be retained for a duration defined by the local retention policy.
- 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. Measures SHOULD be in place to prevent tailgating.
- Doors to controlled access areas SHALL **NOT** be propped open.
- Everyone in a controlled area SHALL be vigilant while inside and challenge and/or report unidentified persons including persons not displaying identification badges (for more on display badges see Section 6.1.7 Identification Badges.
- Physical access control devices/keys issued to an individual SHALL never be loaned or shared with another individual.
- A person possessing an access control device/key SHALL never use that device/key to allow access to an unauthorized individual.

6.1.4 Access Control for Transmission Medium

- A NG9-1-1 entity SHALL control physical access to information system distribution and transmission lines within a physically secure location.

6.1.5 Access Control for Display Medium

- A NG9-1-1 Entity SHALL control physical access to information system devices.

- A NG9-1-1 Entity SHALL position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing.

6.1.6 Monitoring Physical Access

- A NG9-1-1 Entity SHALL monitor physical access to the information system to detect and respond to physical security incidents.

6.1.7 Identification Badges

Identification badges help to easily identify who does and does not belong. Badges help to increase the safety and situational awareness of employees as well as protecting NG9-1-1 assets. Badges may also have additional functionality such as allowing access to devices and/or areas.

- NG9-1-1 Entity employees, authorized non NG9-1-1 employees, and visitors SHALL be issued an identification badge.
- Employee and authorized non-employee's identification badges SHALL display a picture of the individual the card was issued to.
- The issuance of temporary badges for authorized employees who do not have their official badge SHALL follow local policy and procedures.
- The issuance of a visitor badge SHALL follow local policy and procedures.
- Individuals with visitor badges SHALL be escorted while within non-public areas.
- Visitor and temporary badges SHALL be easily and clearly identifiable.
- Identification badges SHALL be prominently displayed while within NG9-1-1 Entity premises.
- If entry points are staffed, identification badges SHALL be presented to the individual at the entry point prior to being allowed in.
- Individuals who do not have an authorized badge or are unwilling to show their badge SHALL be escorted off the premises in accordance with local policy and procedures.
- Visitor and temporary badges SHALL be turned in when leaving a NG9-1-1 facility.
- Lost or stolen badges SHALL be reported as soon as discovered and any access the badge may have allowed disabled within 24 hours of notification.

6.1.8 Visitor Control

- A NG9-1-1 Entity SHALL control physical access by authenticating visitors before authorizing escorted access to any physically secure location (except for those areas designated as publicly accessible).
- The NG9-1-1 Entity SHALL always escort visitors and monitor visitor activity.

6.1.9 Delivery and Removal

- A NG9-1-1 Entity SHALL authorize and control information system-related items entering and exiting the physically secure location.

6.2 Access Control

Access control helps ensure authorized individuals have access to the information and resources they need to accomplish their job and not to information and resources they do not. Access control also helps identify what information and resources may be at risk in the event of an incident.

There are two types of access control: Physical and logical access controls. Physical access controls are discussed in Section 6.1.3 Physical Access Control. Logical access controls limit connections such as access to computers, databases, information, and the internet and are typically controlled with permissions. The recommended way to accomplish this is assigning permissions to groups based on job roles. Then individuals are assigned to the groups required to perform their job functions. This is known as role-based access control.

- Each user SHALL have a unique account.
- All guest and/or anonymous accounts SHALL be disabled.
- Role-based access controls SHALL be used.
- Role-based access controls SHALL be reviewed at least annually.

NOTE: Role based access control allows agency "Policy" to be captured in a standardized format based on XACML as discussed in NENA-STA-010.3 [6].

Access control is often times centrally managed by a single sign-on service. A single sign-on service allows users to authenticate once and access different resources without being required to separately authenticate for additional resources. NENA-STA-010.3 [6] stipulates the requirement of the Security Assertion Markup Language (SAML) that was developed by the Security Service Technical Committee of OASIS as a universal single sign on solution. Please see NENA-STA-010.3 [6] for more information on SAML.

6.2.1 Account Management

The administration of user or entity access and accounts is a major component of the security program. The following outlines the minimum requirements for a NG9-1-1 Entity.

- Creation or modification of accounts SHALL be approved by an authorized representative of a NG9-1-1 Entity.
- Requests for the creation of and/or modification to accounts SHALL be made through an established process that is documented and audited.
- Individuals administrating accounts SHALL ensure that only approved creation or changes to accounts are made.

- The identity of users requesting password resets SHALL be validated before providing any password reset services.

6.2.1.1 Account Change

All changes to accounts are to be made by an authorized account manager or administrator for the resource or information access is being requested for. The authorized representative who authorizes access must have authority for the resource and/or information for which they are authorizing access. This may require multiple account managers/administrators and authorized representatives if the resources/information is controlled by different individuals.

The following actions are taken when a user's job assignment changes (e.g., promotion, demotion, termination, or lateral movement):

- The user's manager SHALL, within one working day, notify account manager(s)/administrator(s) of the change.
- The account manager(s)/administrator(s) SHALL, within one working day of notification, remove access to unauthorized resources and information from the user's account.
- For terminated user accounts or accounts that are no longer needed, the account manager(s)/administrator(s) SHALL, within one working day of notification, disable the user account. The account SHOULD be deleted in accordance with a NG9-1-1 Entity's procedures.
- For a user's account still working for a NG9-1-1 Entity, the user's manager SHALL obtain approval for new access needs from the authorized representative and provide that documentation to the account manager(s)/administrator(s) as soon as possible.
- The account manager(s)/administrator(s) SHALL, within one working day of receipt of the authorization documentation, provide the approved access for the user's account.
- All accounts SHALL be reviewed at least annually for authorized privileges and access.
- Any changes SHALL be reported to the account manager(s)/administrator(s) by an authorized representative.
- Any identified changes SHALL be completed by the account manager(s)/administrator(s) within one working day.

6.2.1.2 All Accounts

- All accounts SHALL have a valid business need.
- All accounts SHALL be approved by an authorized representative.
- All accounts SHALL be checked at least monthly for inactivity.
- All accounts SHALL be reviewed at least annually.

- Unused accounts SHALL be disabled and deleted in accordance with a NG9-1-1 Entity's procedures.
- All accounts SHALL have a unique password that conforms with the Authentication/Password policy.
- All account passwords SHALL be changed in accordance with the Authentication/Password policy.
- Accounts with temporary passwords SHALL require a password change upon first login with the account.

6.2.1.3 Administrator Accounts

Administrator accounts have elevated permissions allowing them to perform actions a normal user cannot. Administrator accounts are powerful accounts that can do many things. They can view information that they have not been granted access to. They can install/delete/modify software, information, and settings. They can add/remove/modify other accounts. There are two general types of administrator accounts. There is a local account that can perform these tasks only on a single device and there are domain/forest level administrator accounts that can perform actions across a NG9-1-1 system.

- Administrator permissions SHALL only be granted to authorized individuals with a valid business need.
- Administrator accounts SHALL only be used to conduct official NG9-1-1 activities.
- Administrator accounts SHALL **NOT** be used for day-to-day user level activities.
- Administrator accounts SHALL only be used to perform an authorized activity requiring elevated permission.
- Local administrator accounts SHALL **NOT** be used when individual domain administrator accounts are an option.
- Non-unique local and domain administrator accounts (i.e., default admin accounts) SHALL only be used during initial installation or under disaster recovery scenarios.

6.2.1.4 Stale Accounts

Stale accounts are accounts that have never been used or have not been used for a while. Sometimes they are accounts for former employees who have left the Entity, sometimes they are accounts that a user never logged into. Often these accounts have simple or default passwords. Stale accounts present an opportunity for an unauthorized individual to gain access to a NG9-1-1 system. Since the account is stale, it can be less likely to be noticed since there is no authorized user that might notice something. An NG9-1-1 Entity needs to periodically check for inactive accounts.

- Accounts that have been inactive for 30 days or more SHALL be reviewed.
- If the accounts are no longer needed or are unauthorized, they SHALL be disabled. The account SHOULD be deleted in accordance with a NG9-1-1 Entity's procedures.

6.2.1.5 Service Accounts

Service accounts are accounts used to perform a specific service. For instance, these accounts may perform automated backup services or perform a database action. These are accounts that don't have an assigned user.

- A service account SHALL **NOT** be used as a user account.
- A user or administrator account SHALL **NOT** be used as a service account
- Each service account SHALL be documented sufficiently to identify what it is used for and where it is used.
- A service account SHALL only have the required permissions and access required to perform the action for which it was made (least privilege).
- Each service account SHALL be dedicated to a single service.
- Service accounts SHALL be prevented from interactive login unless there is a specific business need.

6.2.1.6 Guest / Temporary Accounts

Guest and anonymous accounts allow for unauthenticated access. Anonymous accounts typically do not have passwords and/or usernames associated with them. Guest accounts may have passwords and/or usernames. The intended purpose of these types of accounts on systems or databases is to allow unauthenticated access to non-sensitive information and/or systems.

- Guest and Anonymous accounts on NG9-1-1 networks and systems SHALL be disabled.

6.2.2 Default Credentials and Control of Authentication Credentials

Devices and applications often come from the manufacturer with a default password. These passwords can be easily obtained by bad actors. It is essential that these passwords be changed before placing the device in service.

- New devices and applications that have local accounts SHALL have a new password set in accordance with the Authentication/Password policy for each local account prior to being connected to any system/network.

6.2.3 Login

A login is used to authenticate that a user is who they say they are. This can be accomplished using one or more of the factors of authentication. There are three factors that are generally accepted. These are something you know, something you have, or something you are. There is a fourth factor, which is somewhere you are.

- Access to all systems from external or remote connections SHALL utilize multi-factor login authentication.

- All users of a NG9-1-1 system SHALL be required to authenticate before being allowed access.
- User passwords SHALL **NOT** be visibly displayed when entered.
- Failed authentications SHALL **NOT** identify the reason for the failure.
- After no more than five failed attempts, the user account SHALL be locked out for at least 10 minutes or based on local access policy. An authorized individual may be permitted to unlock an account sooner than 10 minutes if necessary.
- Passwords SHALL **NOT** be hard coded into login sequences or scripts.

6.2.4 Logon Banners

Logon banners are messages displayed to a potential user that must be accepted before gaining access to any resources or data. These messages inform a potential user that the systems may be used by authorized individuals, used for authorized purposes, actions may be monitored and recorded, and that they will adhere to policy and regulations. The potential user must actively consent to this before proceeding. This is typically accomplished by clicking an accept button. Figure 6-1 Example Logon Banner is an example of a banner message. Some devices have limits on what can be displayed. Consult with your legal department or representative on actual verbiage to ensure that the wording complies with local governance.

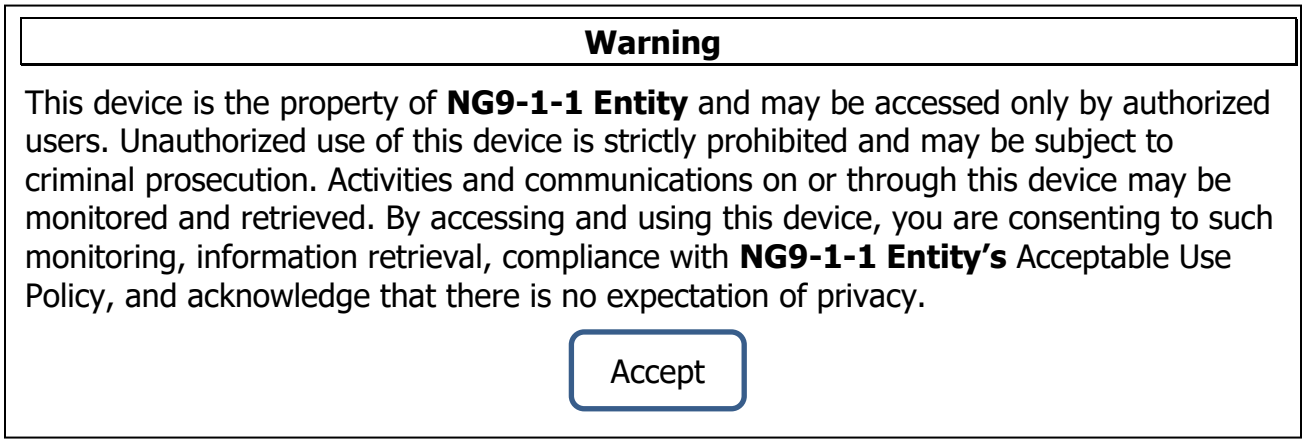

Figure 6-1 Example Logon Banner

- NG9-1-1 Entity SHALL develop legally acceptable banner messages.
- NG9-1-1 Entity devices SHALL display a banner message during the log in sequence.
- The banner SHALL require active acceptance prior to completing the login process and gaining access to any resources or data. Active acceptance requires input from the user.

6.2.5 Passwords/Passphrases

Passwords are the most common form used to authenticate users and validate that they are who they say they are. Passwords fulfill the something you know category of the authentication factors. Knowing this, bad actors have targeted different aspects of the password authentication process. This has generated a change in password requirements over the last few years.

The old method for passwords typically required eight or more characters with a complexity of upper-case letters, lower-case letters, numbers, and symbols. This tends to generate passwords that are hard for users to remember, but easy for computers to crack. Cracking techniques have become more efficient as human behavior is being factored into these cracking algorithms. Paired with faster processing, it has become much faster to crack a password. The predicted time to crack a password varies depending on the source but is generally considered to be less than a day for an 8-character password using full complexity at the time of this writing. This is for a truly random password. Humans do not typically generate truly random passwords. Password cracking will only get faster as algorithms and processing power continue to improve.

The biggest factor in determining how long it takes to crack a password is length. This is where passphrases come in. A passphrase is a group of words put together that is easy for a human to remember but harder for a computer to guess. These words should be words that do not normally go together and should not consist of phrases or words that could be easily determined from social media or other sources of information. A password/passphrase of 12 characters consisting of upper-case and lower-case letters is predicted to take more than a few hundred years to crack depending on the randomness, algorithm, and resources used as of the time of this writing.

- Users SHALL **NOT** use their Passwords/Passphrases for any other account they may have.
- Passwords/Passphrases SHALL consist of 16 or more characters.
- Passphrases SHALL consist of a minimum of three different words or word segments. These should be words that do not typically go together.
- A Passwords/Passphrases SHALL consist of upper-case letters, lower-case letters, numbers, and symbols.
- Passwords/Passphrases SHALL **NOT** consist of sequential characters or words that repeat three or more times.
- Passwords/Passphrases SHALL be changed if they are expected to have been compromised.

Mandatory passphrase changes should be removed, or the frequency interval extended to help prevent bad password hygiene. Passphrases should be checked to verify that they do not consist of a dictionary word (any language), are a commonly used password, contain

repetitive or sequential characters, or contain words easily associated with an individual, job, or function.

An effective defense against Brute Force attacks is a well-established password creation policy that includes attempt limitations and clear storage rules (e.g., don't write passwords down where they can be used by others).

More information on user authentication and passwords can be found in NIST SP 800-63B, *Digital Identity Guidelines, Authentication and Lifecycle Management* [24]

6.2.6 Password Manager

Password managers help users maintain and manage multiple passwords. When using a password manager, users only have to remember the password to their password manager. The password for the password manager should be a unique passphrase of 20 or more characters. Password managers should be periodically backed up in accordance with a NG9-1-1 Entities backup plan.

- Only password managers approved by the Security Manager SHALL be used.
- Multi-factor authentication SHALL be required to gain access to any password manager.
- A user's password manager SHALL **NOT** be shared with another user.
- Users SHALL report the loss or suspected compromise of a password manager within one working day of discovery.
- All passwords stored on a lost or potentially compromised password manager, or password manager's database, SHALL be changed within one working day of discovery.

6.3 Device Connectivity

For a device to be on a NG9-1-1 system it must connect. This may be accomplished in one of two ways. It can be a physical connection like connecting an ethernet cable to the Network Interface Card (NIC) or an electronic connection by using Wi-Fi, Bluetooth, 4G, 5G, or some other form of wireless connection. All connection processes need to be authorized, documented, and secured.

- A NG9-1-1 Entity SHALL maintain current documentation on all connections to their NG9 1-1 system.
- All connections transporting sensitive information SHALL be secured (e.g., CJIS, HR, NGCS, CHFE).

6.3.1 Multi-Homed Host

A host is a device that communicates with other devices on a network. This includes things like computers, laptops, tablets, phones, servers, etc. It does not include devices that transport or route network traffic like switches, routers, and firewalls. A multi-homed host

has 2 or more active connections to other hosts. This could be through multiple physical connections, multiple wireless connections, or using both physical and wireless connections. To accomplish this a host must have any combination of two or more physical and/or wireless connections.

Multi-homed hosts introduce the risk of potentially allowing malicious activity to more easily spread between different networks or segments. Multi-homing should be avoided. When there is a need to connect a host to two or more networks/segments, an appropriately configured firewall should be used when the connection bridges two or more network/segments. Sometimes multi-homing has a valid business need. This can often be seen when creating redundant network connections with call-taking equipment.

- If there is a valid business requirement for a host to be multi-homed, the implementation SHALL be approved, documented, have adequate security measures in place, have appropriate logging, and be monitored. Adequate security measures would entail security controls like anti-virus, host firewall, IDS/IPS, etc. Logging is covered in Section 5.6.2 Security Event Logging above.

6.3.2 Wi-Fi

Wi-Fi is a wireless connection technology that follows the IEEE 802.11 standard. It allows for host devices to connect to an access point or another device within a range. An access point is an antenna that transmits and receives the signal to and from a Wi-Fi capable host. The range will vary depending on the access point, host device, and what is between them. Care should be taken when setting up Wi-Fi as the signal can often reach beyond the building or area of desired coverage. Wi-Fi connections should not be used with Sensitive Data/transactions without using additional security controls like a secured and encrypted VPN (Virtual Private Network).

If a NG9-1-1 Entity decides to implement Wi-Fi then they SHALL, at a minimum, take the following actions:

- Change default password(s) in accordance with the Authentication/Password Policy.
- Change the SSID(s) from the default to one that is not easily associated with the device or a NG9-1-1 Entity (consider hiding non-public SSIDs).
- Disable device management over Wi-Fi.
- Use WPA2-PSK-AES (current standard as of this writing) or stronger standard with a strong password in accordance with the Authentication/Password Policy.
- Use a different SSID and WPA2 password if using a Guest network, and ensure it cannot connect to (air gapped from) a NG9-1-1 network.

6.3.3 Other Wireless

Other wireless, in this case, consists of short-range wireless, excluding 802.11, that connects two devices. These ranges are usually from a few centimeters to a few meters.

Actual range will depend on the technology, the strength of the transmitters and receivers, and any interference between them. The most common ones seen currently consist of Bluetooth, Infrared (IR), Near Field Communication (NFC), and Radio-Frequency Identification (RFID). There are more. These communication methods are unsecured and generally rely on their short range for any sense of security.

- NG9-1-1 Entities SHALL ensure that devices that contain or process sensitive information are prevented from transmitting that information through any of these unsecured technologies.

6.3.4 Broadband Cellular

Broadband cellular is the technology used for connecting cellular enabled devices like cell phones and some home monitoring systems. This technology can be used to transfer data and could potentially be used in a NG9-1-1 system depending on the available service at the location. Broadband offers some protection as the tools necessary to break into it are not as readily available as they are for Wi-Fi. This only provides slightly better security as these tools are available and only require a slightly greater skill set to utilize. Broadband has encryption that can offer some protection, but this encryption is a bit dated so may not be as secure as it once was. Like with Wi-Fi, it is recommended that a secure and encrypted connection be used. Some examples of this are a VPN or the use of TLS.

- If a NG9-1-1 Entity incorporates broadband cellular they SHALL ensure the connection has appropriate security.

6.3.5 Peer-to-Peer

Peer-to-Peer (P2P) networking should be avoided. However, there could be some legitimate business uses. For example, operating systems and programs leveraging P2P to facilitate updates to help speed up delivery and reduce external bandwidth utilization.

- P2P SHALL only be allowed for those programs or applications that cannot achieve their legitimate business purpose or mission in any other way.
- If P2P is allowed, a NG9-1-1 Entity SHALL ensure there is a control in place to validate and verify the information.
- If P2P is allowed, a NG9-1-1 Entity SHALL limit the P2P sharing to a NG9-1-1 domain.

6.4 Domain Naming System (DNS)

Domain Naming System (DNS) is used to convert human readable names into IP addresses that devices use. This could be devices or resources on a NG9-1-1 network or any other publicly accessible network. DNS is an essential part of every network and without it access to resources would be limited or nonexistent. DNS follows a hierarchical structure that is geographically distributed throughout the world.

DNS can be targeted by malicious activities. An example of this is implementing a DoS attack against DNS. A DoS attack on DNS can disrupt or prevent access to resources by preventing a DNS server from providing the needed addressing information. Another example of malicious activity involves a malicious DNS service spoofing the identity of a legitimate DNS servicer and providing incorrect addressing and/or blocking addressing information from being provided. Another example involves implementing unauthorized updates that alter legitimate addressing information stored on the DNS server.

Use security controls to help protect DNS servers such as:

- **Domain Name System Security Extensions (DNSSEC):** DNSSEC utilizes digital signatures to verify the identity. Information containing invalid or missing digital signatures is ignored. Clients (computers) can be configured to request DNSSEC validation.
- **DNS logging:** DNS logging can be used to detect tampering and used for other purposes depending on the information captured. DNS logging can impact server performance. There are different debug logging options. One common option is DNS debug logging. DNS debug logging captures a lot of detail and will have a greater impact on server performance than DNS logging. Other options may be available depending on your operating system.
- **DNS cache locking:** DNS cache locking prevents tampering with a recursive DNS server's DNS cache. To improve performance, a recursive DNS server will keep searches for a specified amount of time called a time to live. Further inquiries will use the cached information instead of performing a new search. This is much faster. To prevent tampering with this cache it can be locked. This is typically expressed as a percentage of the time to live. Once the time to live has expired, the record is no longer used.
- **Response time limits:** Response time limits can be set to help protect DNS from various DoS types of attack. When response time limits are set, a DNS server keeps track of the number of times it has responded with the same answer to the same requestor. Once the response time limit threshold has been reached the DNS server takes longer to respond.

For more information, please see NIST SP 800-81-2, *Secure Domain Name System (DNS) Deployment Guide* [25].

- NG9-1-1 Entities SHALL enable DNSSEC on all network DNS servers.
- NG9-1-1 Entity clients SHALL request DNSSEC validation.
- NG9-1-1 Entity zone transfers SHALL be restricted to only authorized servers. This SHOULD be accomplished through access control lists.
- NG9-1-1 Entity DNS servers SHALL have DNS logging enabled.
- NG9-1-1 Entity DNS servers SHALL have the DNS cache locked and set to 100% of time to live.

- NG9-1-1 Entity DNS name servers SHALL have response time limits set.
- Primary DNS servers SHALL **NOT** be publicly accessible.
- Only authorized administrators SHALL have access to primary DNS servers. This SHOULD be accomplished through access control lists.
- Publicly accessible DNS servers SHALL be authoritative-only.
- All accounts with privileged access to DNS SHALL follow administrative account requirements. See Section 6.2.1.3 Administrator Accounts.
- All NG9-1-1 Entity DNS servers SHALL follow patching and updating requirements. See Section 5.5 Patching and Updating.

6.5 Rights & Privileges

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

- 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 privilege, on the other hand, grants or denies access to an object or resource. This could allow a user to see only their files while allowing management to see all of the files.

It is also important 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.)

The following are requirements associated with rights and privileges:

- Access to data SHALL be limited only to those whose roles require access.
- Privileged access to Sensitive Data SHALL only be given to those with a valid need to know.
- Users SHALL only be given the minimum permissions necessary to perform their job, also known as the principle of least privilege.
- Role based access SHALL be used to assign rights and privileges and SHALL be documented.
- At a minimum, an annual audit of users SHALL be conducted to determine what their effective rights and privileges are (e.g., if a user is a member of several security groups it is possible for that user to have privileges that were not intentional).

6.6 Inactive Sessions

An inactive session is one in which an application or device receives no input for a period of time. This period of time where no input is detected is called inactive time and, in most

systems, can have a limit set. Once the inactive time limit is reached the device or application initiates an action usually locking or disconnecting the session. An example of this is a screen saver that comes on after a period of time. These screen savers then require reauthentication to regain access.

- The inactive time limit SHALL be set to 15 minutes or less.
- All devices not in a controlled access area where only trusted users are able to access the device SHALL have a method in place to lock out or terminate an inactive session when the inactive time limit is reached.
- Once a device is locked or disconnected, reauthentication SHALL be required to reestablish the session or gain access.

6.7 Device Protections

Device protections help protect NG9-1-1 system assets from loss, compromise, or damage. These could be from things like natural disasters, connection of unauthorized devices, the physical loss of Sensitive Data as well as attacks from within the network.

6.7.1 Remote Access Device Security

Mobile devices are becoming more prevalent, allowing employees to work from within or outside of their offices. These devices are easily portable and may contain sensitive information. Some mobile devices only have a single account for all users and may not require authentication or only require a simple PIN number to access.

- Personal devices SHALL **NOT** be connected to a NG9-1-1 system in any way (i.e., charging a phone or plugging in a personal USB).
- Remote access devices that store sensitive information SHALL be encrypted in compliance with Section 4.2.2.6 Safeguarding Sensitive Electronic Information.
- Remote access devices SHALL **NOT** be plugged into unauthorized USB charging ports or devices.
- Remote access devices SHALL use an Entity approved connection using TLS, or optionally VPN when systems require the kind of address access limitations a VPN provides.
- Remote access devices that store sensitive information or have access to a NG9-1-1 system SHALL require domain authentication in accordance with the Authentication/Password policy.
- Remote access devices that store sensitive information or have access to a NG9-1-1 system SHALL be powered off, secured, and concealed from view when left unattended outside of controlled and secured areas.
- Remote access devices that store sensitive information or have access to a NG9-1-1 system SHALL **NOT** be left logged in while not in direct physical control of the authorized user who is logged in.

For additional guidance on securing mobile devices, please see NIST SP 800-124 Rev 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* [26].

6.7.2 Environmental Controls

Environmental controls vary by geographic area. These help to protect against natural disasters like fires, floods, earthquakes, heat, cold, and storms as well as disruptions in supply chain resources like power, gas, and water. Environmental factors impact overall system security and human safety. Therefore, environmental factor assessment and mitigation is critical and must be part of an overall NG9-1-1 system security and safety plan. Care should be taken when choosing what environmental controls are used. For instance, sprinkler systems are a common control for fire, but water and electronics do not mix well. Additional controls may be needed such as cutting power to systems when the sprinkler system activates or having established procedures to protect electronic equipment in the event of inadvertent sprinkler activation.

For more information, see NIST SP 800-12 Rev 1, *An Introduction to Information Security* [27].

- NG9-1-1 Entities SHALL identify potential environmental risks for each geographic area.
- Each geographic area of a NG9-1-1 Entity SHALL have environmental protection(s) in place for each identified environmental risk. This would include controls like sprinklers, dust filtration, and HVACs.
- A NG9-1-1 Entity SHALL have documented safety plans for each environmental risk. These are plans for events like fire, flood, etc.
- Environmental sensors SHALL be installed and operational that alert personnel when conditions exceed a normal and/or safe operational range. Some examples of these are smoke, temperature, water, and CO2 sensors.
- Fire extinguishers SHALL be easily viewable and accessible from all locations throughout the facility and in accordance with local code.
- An NG9-1-1 Entity SHALL inspect all environmental controls at least annually and in accordance with local code.
- Mission essential NG9-1-1 systems SHALL have surge protection.
- Mission essential NG9-1-1 systems SHALL have a backup battery system.
- NG9-1-1 Entity policy SHALL address the use of food or drink around NG9-1-1 system devices.

6.7.3 Network Infrastructure

Network infrastructure consists of all the hardware and software that make up a NG9-1-1 system. These include things like firewalls, routers, switches, servers, wiring, access points, Private Branch Exchanges (PBXs), etc. These devices, when housed on site, are typically

contained in server rooms and network closets. When assessing the physical security of these areas be sure to look at any drop ceilings or raised floors.

- Physical access to rooms containing network infrastructure SHALL be restricted to authorized individuals with a valid business need.
- Rooms containing critical network infrastructure SHALL have HVAC capable of maintaining temperature and humidity within the range specified by the manufacturer(s) for all equipment within the room.
- Physical access to rooms containing power distribution, backup power, and HVAC SHALL be restricted to authorized individuals with a valid business need.
- Active network jacks connecting to a NG9-1-1 system SHALL only be in physically secured areas.
- Unused network jacks connected to a NG9-1-1 system SHALL be disabled or removed.
- Network transport media that could potentially transport and/or access sensitive information SHALL be selected, located, and installed in such a way as to discourage wiretapping, electronic eavesdropping, or tampering. For example, the use of fiber optic cable, coax, and/or enclosed conduit for cable runs could be used.
- Smoking SHALL **NOT** be allowed in rooms containing critical network infrastructure.

6.8 Denial of Service Defense

A denial-of-service attack involves an attacker attempting to render a resource unavailable. This could be by overwhelming a device's capabilities or by reducing or blocking the flow of traffic. There are different types of denial-of-service attacks. For more information on denial-of-service attacks please see "Understanding Denial-of-Service Attacks" [28] and "Next Generation 911" [29].

NENA-STA-010.3 [6] outlines some requirements for DoS protections.

- NG9-1-1 Entities SHALL have plans to mitigate DoS types of attacks.
- NG9-1-1 Entities SHALL have procedures to handle DoS types of attacks.

6.9 Segmentation

Segmentation involves separating an environment into two or more parts at the Network Domain level. There are different ways to segment an environment. The most extreme is called air gapped where a segment has no wired or wireless connections to anything outside of the segment. An air gapped segment can be useful in certain situations where it is undesirable to have traffic enter or leave the segment. This form of segmentation is rarely used in a NG9-1-1 system as it has no connections to the outside world. In an air gapped segment, everything must be brought in physically through removable media like a USB or a disk. As of this writing, the most common form of segmentation involves logical

separation where traffic in or out of the segment must pass through a single point, typically a firewall.

Segmentation helps stop or slow the spread of unwanted activity, potentially containing damage to a single segment. This helps improve the resiliency of a NG9-1-1 system. Proper segmentation allows separate components to communicate in the ways necessary for the system to function as a whole. With proper ALLOW rules and exceptions employed, greater scrutiny can be achieved when combined with firewall functionality. The advantages of separating network equipment and functional areas via segmentation are tighter controls, improved ability to build custom alerts specific to each segment and minimizing the risk of unauthorized access to internal systems. Lateral infection rarely looks like normal day-to-day traffic and can be mitigated. Segmentation's primary security benefit is the ability to isolate network elements and/or contain incidents, but is only one layer of defense in depth, albeit an important one.

Segmentation can be part of a zero-trust model. This method of segmentation can be done effectively at the endpoint level if the system has the ability to contain a single infected endpoint without the use of a firewall. Micro-segmentation is a more granular approach that divides traffic at the workload/processing level by applying security policies to each workload governing what is allowed.

A NG9-1-1 system may have production and non-production environments. Production environments are systems where devices and software are utilized for their intended purposes. This is where the day-to-day operations occur. A non-production environment is where devices and software are utilized for other than their intended purposes of day-to-day operations. This could be a test environment where software, hardware, and/or patches are tested, or it could be a training environment for call takers and dispatchers.

It is important to separate production environments from non-production environments to prevent unintentional or malicious activity from entering a production environment from a non-production environment.

- Production environments SHALL be segmented from non-production environments in such a way as to protect production environments from activity in non-production environments.
- Production environments SHALL **NOT** contain development tools.

6.10 Firewalls

Firewall functions monitor traffic passing through them and allow or deny that traffic based on a set of user-defined rules. They typically sit at the edges of a network, at the border of network segments, and on host systems. As perimeter defense, firewalls are important but MUST NOT be relied upon to provide the sole protection. Rather, the systems inside the network must be intrinsically secure, with the firewall providing an additional layer of protection. In some cases, firewalls can be bypassed in an attack. Inside attacks, often

enabled by a phishing attempt or other compromise of an individual or system have become a more commonly observed attack for which firewalls may not provide protection.

Firewalls may also provide visibility into the traffic passing into and out of the firewall depending on what has been configured. This helps in troubleshooting network issues as well as forensic analysis in the event of attack.

There are different types of firewalls. Basic firewalls, called packet filter firewalls, look at packets passing through and act based on information in those packets like IP addresses and port numbers. These firewalls are fast, but do not check the payload. More advanced firewalls, like a Web Application Firewall (WAF), look at all layers of the protocol stack. For more information on firewalls, see NIST SP 800-41 Rev 1, *Guidelines on Firewalls and Firewall Policy* [30].

6.10.1 Next Generation Firewalls

Next generation firewalls combine the functionality of packet filtering, stateful inspection, and proxy firewalls along with other security functions. Next generation firewalls commonly perform behavior-based and/or signature-based deep packet inspection. This extra functionality may include antivirus, traffic and application filtering, traffic monitoring, IDS, IPS, or other network or security functions. Actual functionality will vary so care must be taken when selecting a next generation firewall to ensure it will meet the desired expectations. Next generation firewalls can be part of a unified threat management implementation. Unified threat management combines different security functions. Next generation firewalls provide a high level of security but are not generally sufficient to secure a SIP session. In order to effectively secure SIP a Session Border Controller is required.

6.10.2 Session Border Controller

A Session Border Controller (SBC) is a security element that operates similarly to a firewall, but the SBC is primarily designed to handle SIP and media. Traditional firewalls can only allow or block SIP traffic whereas an SBC can anchor SIP signaling and media. The SBC can act as a gateway to manipulate a session to translate between formats allowing different devices to communicate. SBC's can inspect the session and apply security policies. As with other firewalls, as perimeter defense, SBCs are important but are not to be relied upon to provide the sole protection. Rather, the systems inside the network must be intrinsically secure, with the SBC providing an additional layer of protection.

- A NENA standard Border Control Function consists of a Session Border Controller and SHOULD include Next-Generation Firewall functionality and SHALL be implemented in NG9-1-1 systems at the ingress and egress of the ESInet and MAY be implemented by any entity.

- A Session Border Controller (SBC) SHALL be implemented to protect all real-time (voice, video, etc.) communications.
- All NG9-1-1 entities SHALL deploy a Next Generation Firewall or SBC at all ingress and egress points not just in the ESInet.
- All entry and exit points for each segment within a NG9-1-1 system SHALL have a Next Generation Firewall or SBC.
- All necessary traffic SHALL be identified and documented for each Next Generation Firewall or SBC.
- All firewalls SHALL explicitly block unnecessary traffic.
- All firewall configurations SHALL be reviewed at least annually.
- Firewall patches and updates SHALL be reviewed at least monthly and applied as soon as possible.
- All NG9-1-1 Entity firewalls SHALL have their times synchronized.

Firewalls can log events that are good indicators of a compromise to a system or to evaluate an audit trail. To aid in reviewing logs from multiple devices, logs should be centrally managed. Depending on the number of devices generating logs, this can result in a lot of data to go through. Having an automated process to review these logs is advisable. See Section 5.6.2 Security Event Logging for more on this.

- Firewall logs SHALL be enabled and, at a minimum, record the following:
  - Date/time stamp
  - Unsuccessful firewall logins
  - Successful firewall logins
  - Firewall login disconnects
  - Traffic addressed to the firewall
  - Firewall being stopped, started, or restarted
  - Firewall configuration changes
- Firewall logs SHALL be reviewed daily against an established baseline.
- Firewall logs SHALL be kept for a minimum of 1 year and in accordance with local regulations.
- Firewall logs SHALL be protected from unauthorized deletion or modification.

6.11 External Connections

The operations of NG9-1-1 require external connections to meet the business needs of 9-1-1. This may be to an ESInet, EMS, Fire, Police, state/local networks, or connections to other networks and/or resources. There may be others. 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 during transit over an approved secure connection. Please note that this does not preclude additional security controls within the NG9-1-1 system. For more information, please see Appendix A – Zero-Trust Architecture.

- External connections SHALL operate off the zero-trust model. For more information on zero-trust see Appendix A – Zero-Trust Architecture.
- External connections SHALL be protected with a firewall in accordance with Section 6.10 Firewalls.
- External connections transporting sensitive information SHALL be protected with encryption in accordance with Section 4.2.2.6 Safeguarding Sensitive Electronic Information.

6.12 Demilitarized Zones (DMZs)

Certain applications and services may require accessibility from external networks. These external networks are often untrusted. A common example of this is a website. These applications and/or services need additional protection and are commonly placed on a special, external network segment called a Demilitarized Zone (DMZ). A DMZ provides a more secure environment for interaction with external domains by limiting or blocking access to internal resources with a firewall.

- Externally accessible resources not protected by other means SHALL be placed in a DMZ.

6.13 Defense in Depth

Defense in Depth is an approach that layers together a series of security mechanisms and controls throughout the network to protect the confidentiality, integrity, and availability of the entire system. These layers overlap in such a way that if one security mechanism or control fails, another can provide the necessary security. This provides security redundancy.

Some areas for consideration for Defense in Depth include the following:

- Access (physical and digital)
- Workstation defenses
- Data protection
- Perimeter defenses
- Network and traffic separation
- Monitoring and prevention
- Vendor diversity

Each of these performs a different function while backing up the other.

- Critical systems and sensitive information SHALL utilize Defense in Depth.

6.14 Network Availability

Network availability is accomplished with duplication of hardware and/or software for mission critical functions. It can also include duplication of circuitry within a device such as control boards, power supplies, etc. Adequate redundancy can help avoid outages that

impact availability based on single hardware failure events. Typically protocols such as Virtual Routing Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP) are used to provide automated transfer of traffic between banks of equipment during failure events.

Traditional local High Availability (HA) in IP space can be handled by multiple elements:

- Fast-action STP/RSTP/PVST+ re-converging redundant LAN switches or stacked LAN switches
- Teamed NICs in servers and mission-critical desktop computers
- Redundant servers
- HA firewalls
- Redundant routers
- Redundant WAN links
- Out-of-band (OOB) communication links
- Redundant premise wiring
- Separate power feeds
- 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. Network redundancy should be considered when implementing NG9-1-1 networks. See NENA-STA-010.3 [6] for more on redundancy.

- Critical NG9-1-1 systems SHALL have redundancy to ensure the availability of mission critical functions.

6.15 Diversity

Security is primarily concerned with availability in relation to diversity. Diversity requires the use of physically separate routing and cabling to provide protection against outages triggered by a single event. Network diversity can be difficult and expensive to design and implement, however, it is warranted when a very high degree of availability is required. The necessary amount and nature of physical separation needs to be clearly understood and defined. Such separation may range from simple measures such as dual cable entrances on opposite sides of a building to far more complex solutions such as different data centers in geographically diverse locations not typically subject to the same environmental hazard.

Use of redundancy and/or diversity can influence various types of security products. Most notably, traffic failovers between different locations and different firewall sites could result in dropping sessions which are underway at the time of the failover. Applications need to be designed to elegantly recover from such events.

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

- 9-1-1 call traffic SHALL enter a NG9-1-1 system through diverse paths.
- Critical NG9-1-1 systems SHALL have diversity to ensure availability of mission critical functions.

6.16 Traffic Separation

To protect the security, reliability, and maintain efficiency of different segments of a NG9-1-1 network it is important to separate traffic. There are different types of traffic within a NG9-1-1 network. These can differ from Entity to Entity depending on the roles and functions assigned to the Entity. Some possible examples are call traffic, management traffic, IT traffic, HR traffic, and administrative traffic. This separation helps preserve the confidentiality and integrity of the traffic and helps reduce the ability of malicious activity to propagate. There are different ways this can be accomplished. It can be accomplished virtually through VLANs or through physical separation using dedicated equipment. Traffic in and out of these segments needs to be filtered using firewalls. See Section 6.10 Firewalls for more on this.

- Management and monitoring of virtual and logical networks SHALL be handled out of band from regular traffic. For example, management and monitoring will use one VLAN while normal traffic flows through another VLAN.
- For virtual separations, normal traffic SHALL **NOT** use the default VLAN.
- Access to configuration settings on devices handling network traffic SHALL utilize an administrator level account. See Section 6.2.1.3 Administrator Accounts.

6.17 Remote Access

Remote access is defined as connecting to a NG9-1-1 system resource that you are not physically at. This can be external or internal. External remote connections present the highest security risk. Examples of remote access include, but are not limited to the following examples:

- Remote connection to a NG9-1-1 system for maintenance purposes.
- Remote connection to the components supporting functions within a NG9-1-1 system (Databases, Routers, Switches, CPE, etc.).
- Remote connection to a NG9-1-1 system to use an application specifically designed for remote use (i.e., mobile call taking software).
- NG9-1-1 users remotely connecting into a NG9-1-1 system.

For more information on VPNs please see NIST SP 800-77 Rev 1, *Guide to IPsec VPNs* [31].

- External remote access SHALL be only allowed for those with a valid business need.
- External remote access accounts SHALL be reviewed at least annually.
- All external remote access connections SHALL be through an authorized secured and encrypted connection like a VPN.
- NG9-1-1 Entities SHALL **NOT** use modems for external remote connections.

- All external remote access connections SHALL require multi-factor authentication.
- Domain or system authentication SHALL be required after successfully establishing an authorized external remote connection but before gaining access to any resources. Note: this means there are two authentications. One to establish the connection and one to authenticate to the domain.
- Inactive external remote connections SHALL be terminated after 30 minutes or less of inactivity.
- A NG9-1-1 Entity SHALL log, at a minimum, all external remote access connections successful authentication attempts, failed authentication attempts, source IP, start of session timestamp, and end of session timestamp.

6.18 Intrusion Detection/Prevention

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) [32] monitor traffic and alert or take actions based on their capabilities and configurations. There are primarily two ways that IDS/IPS are implemented. On a device and on a network. If implemented on a device, it is referred to as a host-based intrusion detection system. If implemented on a network, it is referred to as a network intrusion detection system.

An IDS monitors activity and alerts when detections are made. What they can monitor varies. For example, some can identify suspicious behavior, some can detect security polity violations, and/or some can identify malicious code. When a detection is made an IDS sends alerts to the configured recipients. The typical recipients configured are administrators and/or a SIEM. There are different types of IDS with the most common being:

1. **Signature-Based**

   Signature-based detection looks at patterns and compares those to known bad signatures in its database. This is similar to the way anti-virus software works; however, an IDS can also identify other events or activities. For instance, an IDS may be configured to detect acceptable use policy violations, large file downloads, or specific email attachments. The additional capabilities available will depend on the IDS. Signature-based detection is the simplest method and only works against known threats.

2. **Anomaly-Based**

   Anomaly-based detection looks at the deviations from normal. Anomaly-based detection needs to first understand what normal looks like and this needs to be adjusted over time as things change. There are two types of anomaly-based systems. One that has static profiles and one that has dynamic profiles. Static profiles need to periodically have the profiles updated. Dynamic systems automatically adjust their profiles. Anomaly-based detection works well against unknown threats. The weakness is if an attacker starts out performing minimal

activities and slowly increasing over time the activity may become part of what normal looks like and not identified. Anomaly-based detection may also flag infrequent events as they are outside of what it knows as normal.

An IPS is an IDS with the additional capabilities to perform automated responses that can change, alter, or block connections. The response varies and depends on the capabilities and configuration of the device. 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 if intrusion prevention technologies are implemented, they be managed by a knowledgeable security professional.

For more information, see NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* [32].

- If a signature-based IDS/IPS is used the signatures SHALL be updated at least weekly. More frequent updates are recommended.
- If an anomaly-based IDS/IPS is used the profiles SHALL be updated at least annually. More frequent updates are recommended as needed.
- Alerts SHALL be reviewed at least weekly.
- Configurations SHALL be reviewed at least annually.

6.19 Endpoint Security

An endpoint is a computing device that communicates with one or more other devices that may or may not be on a NG9-1-1 network. These are things like computers, smartphones, tablets, internet-of-things devices, or network components like firewalls, routers, switches, gateways, or sensors. In essence, everything that is plugged into or connected to a NG9-1-1 system that has some sort of processing capabilities. Endpoints are what allow a NG9-1-1 system to function, employees to accomplish day-to-day activities, and, unfortunately, where malicious actors perform their actions.

Hardening an endpoint decreases the risk that an endpoint will be exploited. Device hardening may help protect against threats such as URL manipulation attacks, input validation attacks from within, denial of service attacks, brute force attacks, session hijacking, clickjacking, port scanning, etc.

Hardening endpoints involves deleting or disabling programs, applications, ports, protocols, drivers, etc. that are not required. It also involves things like updating and patching the device's firmware and software, access controls such as restricting permissions to system files and data, encrypting storage, logging, following robust authentication and authorization for all services, active threat monitoring, and ensuring implementation of modern endpoint protection software. In essence, only allow what is needed for the device to perform its intended function and delete or block everything else. This takes time, and

when possible, should be performed on a master image that can be replicated to other similar devices.

It is important to note that backup and recovery procedures are separate from hardening, but they are equally important and should not be overlooked. See sections 5.7.2 System Backup and Restoration and 4.3.2.4 Examples of Mitigation Techniques for details.

Endpoint protection software implements safeguards to protect devices against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.).

For more information on endpoint protection software see NIST SP 800-128

https://csrc.nist.gov/pubs/sp/800/128/upd1/final.

For operating systems and applications, a good place to start the hardening process is to see if a security checklist is available. This guidance is called a STIG, which stands for Security Technical Implementation Guide. STIGs were developed by the Defense information Systems Agency to help protect DoD systems. NIST provides STIGS for various operating systems and applications at https://ncp.nist.gov/repository?sortBy=modifiedDate%7Cdesc. To view these, you will need a STIG viewer. The DoD provides a free publicly available STIG viewer that can be downloaded from https://public.cyber.mil/stigs/stig-viewing-tools/.

- Endpoints supporting mission critical functions SHALL be hardened.
- Endpoints supporting mission critical functions SHALL be reviewed at least annually to ensure they are still hardened.

6.20 Email

Email presents a security risk to a NG9-1-1 system. It has become one of the primary vectors for phishing campaigns, spreading malware, and can be used by unauthorized individuals to gain access. Emails can be used to trick recipients into divulging sensitive information, stealing funds, execute malicious code, or other undesirable actions.

One of the best security controls for email is Security Awareness Training. Security Awareness Training (see Section 5.1.1 Cybersecurity Awareness Training) provides the training for NG9-1-1 staff in how to recognize, avoid, and report email phishing attempts. Properly trained staff can often catch suspicious emails better than security controls.

The other part of protecting email is the mail server. A mail server may be on premises, hosted, or a hybrid of both. On premise mail servers are maintained and managed by a NG9-1-1 Entity while hosted mail servers are typically maintained and managed by a hosting entity. It is important to ensure that mail servers are securely configured and hardened.

Email is often used to spread malware. Scanning email for malware helps reduce the likelihood of malware entering or leaving a NG9-1-1 Entity. Email can be scanned at different points. It can be scanned at a firewall, mail relay, mail gateway, mail server, or at the user's workstation. There are strengths and weaknesses with each. It is recommended that email be scanned at the user's workstation and at one or more of the other locations.

Email can also be filtered by content. Content filtering can tag, quarantine, delete, clean, or block messages containing specified types of content. This content could be spam, executables, code/script, specific file types, and/or specific words. Often, content filtering is performed in conjunction with malware scanning.

For more information on how to secure email please see NIST SP 800-45 Ver 2, *Guidelines on Electronic Mail Security* [33].

- Mail server(s) SHALL be installed on a dedicated system or systems.
- Mail server(s) SHALL be hardened.
- Email SHALL be scanned for malware.
- Email SHALL have content filtering.
- Call taking workstations SHALL **NOT** be used to send/receive/view email.

6.21 Text, Pictures, and Video 9-1-1 Communication Data

The ability to text 9-1-1 is becoming increasingly common. Many NG9-1-1 Entities now accept text. Viewing texts normally does not pose a threat. Clicking on links in a text can pose a threat. As capabilities increase, photos, and video may become more available. Photos and videos can have data embedded in them through a process known as steganography. Steganography requires specialized software or code to access that data. An example of this uses a process called "Stegosploit." This process hides code in a photo that is then executed when viewed by a browser using a webpage specifically configured to load the photo. This is not something that would typically be done by a NG9-1-1 Entity to view photos. Other techniques could eventually come along that a NG9-1-1 Entity would be more susceptible to.

Texts, photos, and videos come from untrusted sources and call taking systems need to be protected from potential malicious activity from these vectors. One approach to doing this is to use secure sandboxes or similar container-like environments. These secure containers create a virtualized environment that is isolated from the host system and other trusted resources.

- A NG9-1-1 Entity viewing text messages to 9-1-1 SHALL define how to handle links in 9-1-1 requests.
- Text, pictures, and video SHALL be opened/viewed in a manner that protects critical NG9-1-1 system resources from malicious content.

6.22 Encryption

Encryption is the process of securing data in such a way that only individuals with the correct encryption key can view the data. An encryption key is a long string of characters like a password that can be used to encrypt or decrypt. Depending on the encryption method used, this may be a single key like in symmetric encryption or a special key pair like in asymmetric encryption. The security of the encryption depends on the algorithm used and the length of the key. Computers are capable of cracking passwords given enough time. The amount of time depends on the processing power of the computer, length of the key, and strength of the algorithm used. Over time flaws are found in algorithms or the processing power increases to a point that renders the key length obsolete. It is important to ensure that the algorithm used, and the length of the key selected are sufficient to protect the data for the length of time that data needs to be protected.

For more information on encryption, see NIST SP 800-175B, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms* [34].

- NG9-1-1 Entity SHALL use a security algorithm as specified in NENA-STA-010.3 [6].
- NG9-1-1 Entity encryption algorithms and key lengths SHALL be selected such that they are expected to protect that data for the duration the data needs to be protected.

6.23 Cryptography

Cryptography is used to protect data and/or validate identity and relies on an algorithm and a key or key pair. Algorithms are complex mathematical processes that change over time as new ones are developed and old ones become compromised. Two types of algorithms are commonly used today: Symmetric key algorithms and asymmetric key algorithms.

Symmetric key algorithms are less resource intensive and used to protect data. In symmetric key algorithms, the same key is used to encrypt and decrypt. Since there is one key, everyone and everything authorized to have the key must protect the key. A compromise anywhere along the way can lead to a potential compromise of the data.

Asymmetric key algorithms are more resource intensive than symmetric encryption and can be used to protect data and/or validate identity. Asymmetric encryption relies on a special key pair. One key is referred to as the public key, and the other as the private key. This pair of keys operate in a special way that only allows data encrypted with one key to be decrypted by the other. This special relationship can be used to prove identity or protect data and only provides security as long as the private key is kept private. To prove identity, the owner of the key pair encrypts a small piece of data called a signature with the private key. The public key is then used to decrypt. Identity is proven since only someone who has

the private key can encrypt the signature. To protect data, the public key is used to encrypt the data. Then only the owner of the private key can decrypt it.

When setting up a secure communication channel, it is common to use the asymmetric process first to prove identity for each end and to securely pass a symmetric key. Then the faster symmetric process is used to securely transmit encrypted data between the two endpoints. Once the session is done, the connection is closed, and the asymmetric key is discarded. If a later transaction is needed, a new key is generated.

Cryptography in 9-1-1 primarily deals with securing connections and asserting identity. This generally relies on Public Key Infrastructure (PKI), digital certificates, and Transport Layer Security (TLS). This is managed through the key management process. These concepts are described below.

This section describes the NG9-1-1 PKI. However, the description of the NG9-1-1 PKI in this section is informative. This standard asserts no additional requirements on the NG9-1-1 PKI. The controlling specifications for the NG9-1-1 PKI are the following:

- NG9-1-1 Interoperability Oversight Commission (NIOC) PSAP Credentialing Agency Certificate Policy
- NIOC PSAP Credentialing Agency Certificate Validation Policy
- NENA i3 Standard for Next Generation 9-1-1

These specifications are incorporated into this standard by reference.

6.23.1 Identity

NG9-1-1 has a uniform notion of identity. The i3 standard calls for a (PKI) in which an NG9-1-1 entity's Identifier, Role and Agency Affiliation are conveyed in a validated X.509 digital certificate that shares a root of trust with a shared Root Certificate Authority (CA). In NG9-1-1 the root CA is called the PSAP Credentialing Agency (PCA). The intent of specifying an NG9-1-1 PKI is to allow entities in one agency to have a level of explicit trust when communicating with entities from disparate agencies as they participate in the same security community. This framework is somewhat similar to Certificate Authority frameworks widely used on the Internet, except the PCA is applied to public safety identities. Credentials (conveyed in a certificate) traceable to the PCA are required for many interactions in NG9-1-1 standards including i3.

6.23.2 Public Key Infrastructure

PKI is a framework used to issue, maintain, and revoke digital certificates. It is used to validate identities and/or secure data. It is a process used to generate a verifiable binding of a public key to a specific Entity through a chain of trust. It allows for a level of confidence that the person or process sending the transaction is who they claim to be and the person or process receiving the data is the intended recipient. PKI depends on digital

certificates. The most common place this can be seen today is on the web. The web uses PKI to set up secure connections.

The NG9-1-1 PKI shares a root CA called the PCA. ESInets deploy their own Intermediate Cas (ICAs) that they control and operate. The PCA's role is only to issue certificates to ICAs; ICAs can then issue certificates to additional ICAs or to end-entities like ESInet elements or people. Every CA in a PKI must have a Policy Authority (PA). For interoperability internationally or across different domains, it is possible to cross-sign the PCA with a second root CA, or to issue a bridge CA in collaboration with the second PA. However, cross-signing or bridging PKIs must be done sparingly and with great caution, as both PKIs will share a threat surface and will be bound to each other's rules.

A diagram of the NG9-1-1 PKI is depicted below in Figure 6-2 Public Key Infrastructure.

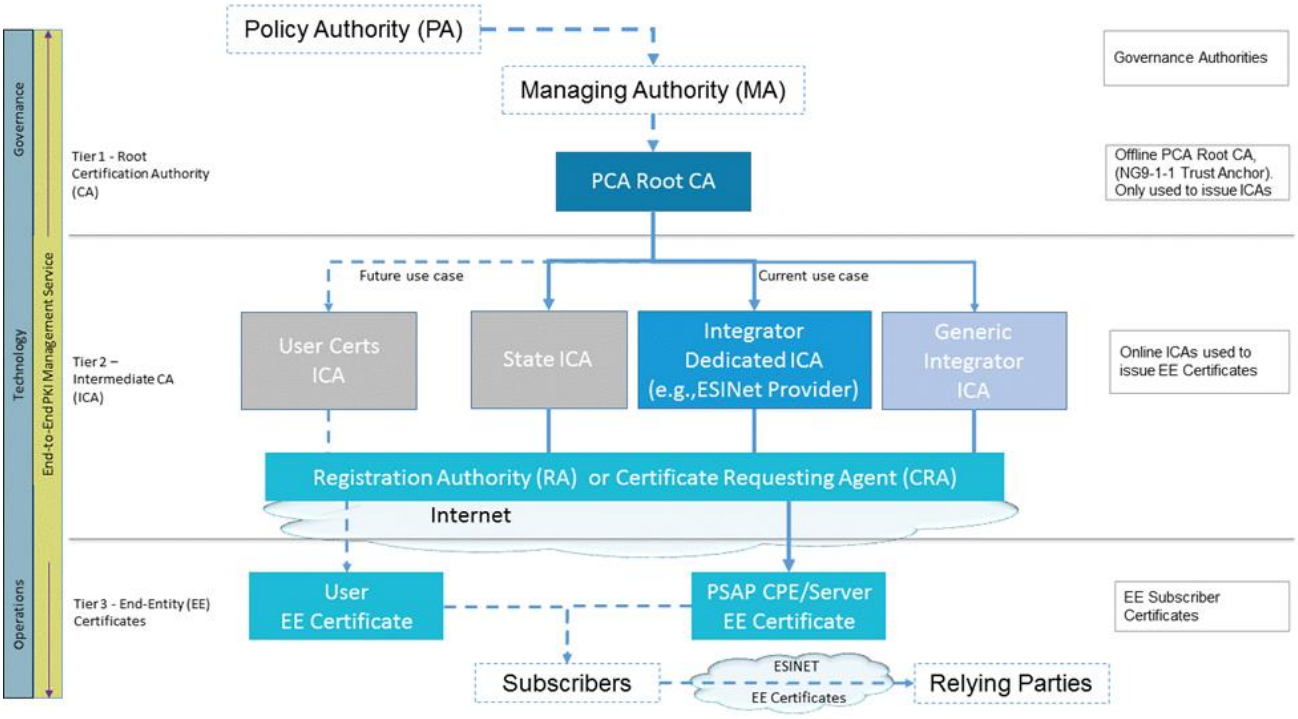

Figure 6-2 Public Key Infrastructure[5]

6.23.3 Digital Certificates

A digital certificate, also known as a public key certificate or identity certificate, is used to validate the ownership of a public key by an entity through a system of trust. The issuer of a digital certificate must be trusted by both ends. The ends can be different devices on the same network or different Entities. In PKI, a Certificate Authority (CA) that is trusted by

[5] Diagram from *Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy v1.1* [35]

both Entities is typically used. A CA verifies the identity of an Entity requesting a digital certificate. This verification may be delegated to a registration authority by the CA. Once a CA has vetted an Entity, they digitally sign a digital certificate and provide it to the Entity. A CA maintains a list of revoked certificates and provides this information to the public. Revocation is a process by which an issued certificate that has not yet expired can be declared invalid. This is typically done when a private key has been compromised.

A digital certificate consists of information about the certificate like its start date and end date along with information about the Entity, the Entities public key, and the CA's digital signature. This information is used in validating the certificate and setting up secure communications. When a digital certificate is used, it is checked to see if the CA is trusted, the certificate is valid, the certificate has not expired, the certificate has not been revoked, and the certificate has not been altered. If it passes, then the public key is used to set up secure communications. As of this writing, the most used certificate format is the X.509 standard.

How an entity's information is included in an NG9-1-1 Certificate is standardized, as is the procedure for validating end-entities (such as PSAP equipment or a telecommunicator) and Issuing Certificate Authorities (ICAs), which are normally operated by 9-1-1 authorities. The documents governing how NG9-1-1 Certificates are issued are controlled by the Policy Authority for the PCA, which is called the NG9-1-1 Interoperability Oversight Commission.

An example of a valid "otherName" element for an agency that processes emergency calls and includes a local police, fire, and EMS function is shown below in Figure 6-3 Digital Certificate Example.

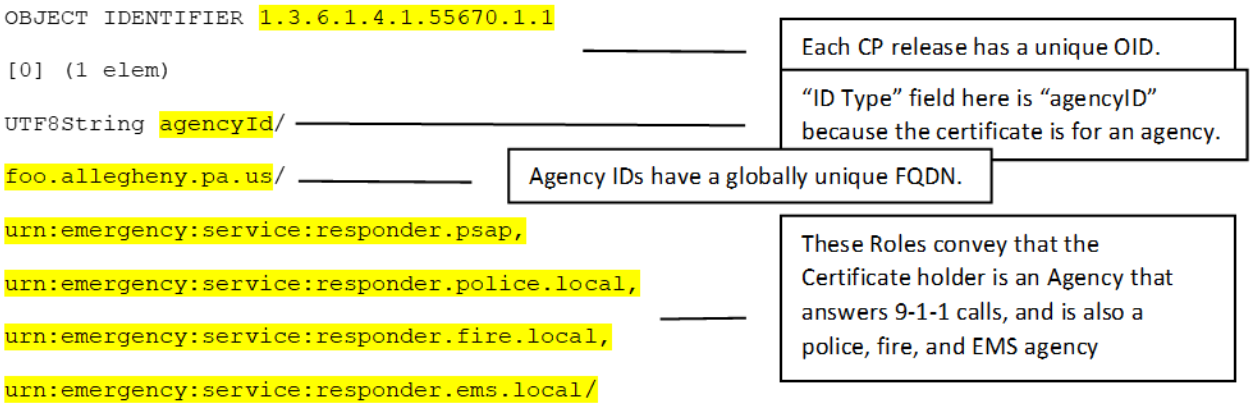

Figure 6-3 Digital Certificate Example

6.23.4 Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol used to secure connections. As of this writing, TLS is the most widely used protocol to secure connections such as email, instant messaging, VoIP, and HTTPS. NENA-STA-010.3 [6] states that all SIP elements must support TLS, that SIP signaling within the ESInet should be over TLS connections, and recommends TLS be supported over all connections that use HTTP.

As of this writing, TLS is the preferred protocol used to establish secure communications. TLS replaced SSL. SSL and the early versions of TLS have become obsolete and no longer provide the security they once did. As of this writing, TLS 1.3 is considered secure and TLS 1.2 is considered secure only if the NULL, RC2, RC4, DES, IDEA, and TDES/3DES encryption algorithms are not used. These encryption algorithms have been removed from TLS 1.3. Care must be taken to ensure that obsolete and/or weak algorithms and/or versions are not used. Devices should be set to not accept connection protocols that are no longer secure. For SIP connections, NENA-STA-010.3 [6] states that TLS should be used with a fallback of TCP than UDP.

In the NG9-1-1 PKI, PCA-traceable credentials are expected to be used for all TLS connections. This allows TLS negotiation not only to establish security, but to assert identity across any elements that are interacting. By having a secure, validated identity, different ESInets and agencies can interoperate more seamlessly as they can trust that both entities are legitimate public safety entities. This also allows elements to grant access based on permissions, such as by public safety discipline or with a specific agency or specific agent.

6.23.5 Certificate Policy and Certificate Practice Statement

Every participant in a PKI is bound to the rules of a Certificate Policy (CP). Every PKI has a CP. The CP describes the architecture of the PKI, rules for issuing certificates, rules for revoking certificates, and other technical and operational aspects of participating in a PKI. For example, generic web certificates used to secure websites are all bound to the CP from the issuer, even if the website is just a personal blog. The NG9-1-1 PCA CP establishes a very high level of assurance. A significant difference in the PCA CP from a standard general-purpose CA is the special way in which the NG9-1-1 PKI handles identity.

6.23.6 Validation

The NG9-1-1 PKI has a special procedure for validation as detailed in the PCA Validation Policy (VP). The purpose of this validation procedure is to prove the identity that will be asserted within a certificate. The NG9-1-1 validation procedure is similar to Extended Validation used for general purpose CAs but is specific to NG9-1-1 and public safety needs. For example, the VP details procedures for validating an agency and its public safety role, legitimate public safety purpose of that agency, an ESInet element's function, a human's affiliation with an agency and other details.

NG9-1-1 Certificates fall into multiple categories and are either CA Certificates credentialing a CA or an end-entity Certificate credentialing an Agency, Service, User, Element, or User. Table 6-1 Allowable NG9-1-1 Certificate Categories, shown below, is a summary of the types of NG9-1-1 Certificates allowable under the PCA CP and VP.

Validation is done by a Registration Authority (RA) for a given CA. Every CA has an RA. The RA for the PCA is designated by NIOC, the entity that is responsible for the PCA. The RA for an ICA is designated for that ICA; for example, an ICA for a statewide ESInet may assign a state agency to serve as an RA. An RA can then designate a Local RA (LRA); for example, the statewide RA may designate LRAs in regions of the state or individual counties. This allows great flexibility in how each leg of the PKI is operated without compromising security, as each RA and LRA is thoroughly vetted by an existing RA.

Table 6-1 Allowable NG9-1-1 Certificate Categories

Type of Cert	Description	Validation Done By
Root Certificate	The PCA's offline root certificate that is the basis of the trust chain for the NG9-1-1 PKI	Self-signed by the root CA in an auditable ceremony per the CP
ICA Certificate	A certificate for an ICA	The RA for the CP for a Tier-2 ICA, or the RA in the CPS governing the signing ICA

Type of Cert	Description	Validation Done By
Agency Certificate	A certificate issued to an agency. ID example: psap.fairfax.virginia.us	The RA for the ICA
Service Certificate	A certificate issued to a service instance in a particular NGCS or Agency	The RA or LRA for a CA with Delegated Authority to perform Validation
Element Certificate	A certificate issued to a physical or virtual entity that is addressable and has a unique identity (elementID)	The RA or LRA for a CA with Delegated Authority to perform Validation.
User Certificate (Agent)	A certificate issued to a person or automaton. These are always issued by an ICA. ID example: dhandy@psap.fairfax.virginia.us	The RA or LRA for a CA with Delegated Authority to perform Validation

There is significant power associated with an Agency Certificate. This is because an Agency Certificate is required to sign a Certificate Signing Request (CSR) for any end-entity certificate (such as for an ESInet functional element, call-handling position, etc.). The fact that an Agency has used an Agency Certificate to sign a CSR for an end entity certificate constitutes much of the validation procedure for end-entity elements. Accordingly, Agency Certificates are subject to a very high level of validation. Additionally, the Private Key for an Agency Certificate must be carefully protected, as a compromise of an Agency Certificate may indicate compromise of the end-entity certificates whose CSRs it has signed.

6.23.7 Cryptographic Keys

Cryptographic keys appear like a very long random string of characters. They are generally unique to each algorithm and can't be interchanged between them. These keys are typically generated by a specialized process that creates a random key normally on the requesting computer. For asymmetric keys, the public key is provided to the CA for inclusion in the digital certificate and the private key is stored in a specified location on the network.

The private keys from the asymmetric key pair and symmetric keys need to be protected from loss, corruption, or unauthorized access. Malicious actors often go after the keys instead of trying to crack encryption as cryptographic algorithms have become harder to compromise. Cryptographic keys that are stored need to be protected with access restricted to only authorized individuals, devices, and/or applications. Periodic reviews need to be conducted to help ensure that only authorized users/devices have access.

Please see the following for more information:

- *Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy V1.1* [35]
- *NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines* [36]
- *NENA i3 Standard for Next Generation 9-1-1* [6]
- *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations* [37]
- *NIST SP 800-57 Part 2 Rev 1, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations [38]*

- Private keys SHALL be classified as Sensitive (Most Sensitive Information).
- Private keys SHALL be protected from unauthorized disclosure.
- Private keys that are compromised or suspected of being compromised SHALL be revoked and new keys issued if needed.
- All requirements from the NIOC's PCA Certificate Policy are incorporated into this standard by reference and SHALL be adhered to by implementations.
- All requirements from the NIOC's PCA Validation Policy are incorporated into this standard by reference and SHALL be adhered to by implementations.

6.23.8 Self-Signed Certificates

Self-signed digital certificates (i.e., digital certificates not issued by a Certificate Authority) MUST NOT be used for any communications that traverse an ESInet. NG9-1-1 Entities, including NGCS and PSAPs, MUST use digital certificates traceable to the PCA Root certificate for NG9-1-1 communications. External entities that do not participate in the PCA-traceable PKI that interact with an ESInet MUST use digital certificates issued by a reputable public Certificate Authority.

- Self-signed digital certificates (i.e., digital certificates not issued by a Certificate Authority) SHALL **NOT** be used within or between ESInets for NG9-1-1 communications.
- External entities that do not participate in the PCA-traceable PKI that interact with an ESInet SHALL use digital certificates issued by a reputable public Certificate Authority.

6.24 Disposal

At some point devices and paper are no longer needed and must be disposed of. These items may contain sensitive information that needs to be disposed of appropriately to ensure that it is not inadvertently disclosed. Please see Appendix A in NIST SP 800-88 Revision 1, *Guidelines for Media Sanitation* [39], that provides the minimum sanitization requirements for various items for more information.

- Paper material containing sensitive information SHALL be disposed of in such a way that it is impractical to reconstruct any portion of a document.

- Devices that never held or processed sensitive information SHALL, at a minimum, be reset to factory defaults with all NG9-1-1 data removed.
- Devices that held or processed sensitive information at any point SHALL have their volatile memory cleared and any electronic storage media sanitized.
- Cloud-based storage SHALL have all Sensitive Data being disposed of rendered irretrievable.

7 Abbreviations, Terms, and Definitions

See the NENA Knowledge Base (NENAkb) [1] for a Glossary of terms and abbreviations used in NENA documents. Abbreviations and terms used in this document are listed below with their definitions.

Term or Abbreviation (Expansion)	Definition / Description
ALI (Automatic Location Identification)	ALI (Automatic Location Identification) is the automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information of the location from which a call originates.
BIOS (Basic Input Output System)	BIOS (Basic Input Output System) stands for Basic Input Output System. It is software stored on a small memory chip on the motherboard used at start up time.
CAD (Computer Aided Dispatch)	A CAD (Computer Aided Dispatch) is a computer-based system, which aids PSAP Telecommunicators by automating selected dispatching and record keeping activities.
CCNA (Cisco Certified Network Associate)	Cisco Certified Network Associate is an information technology certification from Cisco Systems.
CCNP (Cisco Certified Network Professional)	Cisco Certified Network Professional is an information technology certification from Cisco Systems.
Classified Data	Data not controlled by a data rights management system.

Term or Abbreviation (Expansion)	Definition / Description
CJIS (Criminal Justice Information Services)	CJIS (Criminal Justice Information Services) serves as the focal point and central repository for criminal justice information services in the FBI. Programs initially consolidated under the CJIS Division included the NCIC (National Crime Information Center), UCR (Uniform Crime Reporting), and Fingerprint Identification. In addition, responsibility for several ongoing technological initiatives was transferred to the CJIS Division, including the IAFIA (Integrated Automated Fingerprint Identification System), NCIC 2000, and the NIBRS (National Incident-Based Reporting System).
DNS (Domain Name System)	DNS (Domain Name System) is a global, distributed, delegated database of records about domain names. Each type of record holds a specific type of information. DNS is queried with a domain name and desired record type. The response is the record data associated with the queried data. Some records contain an IP address for a domain name, other record types contain email or SIP server information for a domain name, etc.
ECC (Emergency Communications Center)	ECC (Emergency Communications Center) is a facility designated to receive and process requests for emergency assistance, which may include 9-1-1 calls, determine the appropriate emergency response based on available resources, and coordinate the emergency response according to a specific operational policy. Note: The term "ECC" does not have the same meaning as "PSAP."
FIPS (Federal Information Processing Standards)	FIPS (Federal Information Processing Standards) is a standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. FIPS are a set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

Term or Abbreviation (Expansion)	Definition / Description
HVAC (Heating, Ventilation, and Air Conditioning)	The term HVAC (Heating, Ventilation, and Air Conditioning) generally refers to your home, vehicle, or business's heating and cooling system.
IDS (Intrusion Detection System) or IPS (Intrusion Prevention System)	An Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) is either a hardware device or software application that uses known intrusion signatures and/or behavior-based algorithms to detect and analyze traffic.
NCIC (National Crime Information Center)	NCIC (National Crime Information Center) is an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year. It helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. It also assists law enforcement officers in performing their duties more safely and provides information necessary to protect the public.
NG9-1-1 (Next Generation 9-1-1)	NG9-1-1 (Next Generation 9-1-1) is an IP-based system comprised of hardware, software, data, and operational policies and procedures; see https://kb.nena.org/wiki/NG9-1-1_(Next_Generation_9-1-1) for more details.
NGCS (Next Generation 9-1-1 Core Services)	NGCS (Next Generation 9-1-1 Core Services) is the set of services needed to process a 9-1-1 call on an ESInet. It includes, but is not limited to, the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services, and typical IP services such as DNS and DHCP. The term NG9-1-1 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network.
NIC (Network Interface Card)	A NIC (Network Interface Card) is an internal circuit board or card that connects a workstation or server to a networked device.
NIST (National Institute of Standards and Technology)	NIST (National Institute of Standards and Technology) is part of the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Term or Abbreviation (Expansion)	Definition / Description
PBX (Private Branch Exchange)	A PBX (Private Branch Exchange) is a private telephone switch that is connected to the Public Switched Telephone Network.
PSAP (Public Safety Answering Point)	PSAP (Public Safety Answering Point) is a physical or virtual entity where 9-1-1 calls are delivered by the 9-1-1 Service Provider. See https://kb.nena.org/wiki/PSAP_(Public_Safety_Answering_Point) for more details.
PCA (PSAP Credentialing Agency)	PSAP Credentialing Agency is the root authority designated to issue and revoke security credentials (in the form of an X.509 certificate) to authorized 9-1-1 agencies in an i3-compliant infrastructure.
PKI (Public Key Infrastructure)	Public Key Infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
RAID (Redundant Array of Independent Disks)	RAID (Redundant array of independent disks) is a storage device that uses multiple disks to provide fault tolerance, improve overall performance, and increase storage capacity in a computer system.
SAML (Security Assertion Markup Language)	SAML is an XML-based, open-standard data format for exchanging authentication and authorization data between an identity provider and another party.
Sensitive Data	Sensitive Data is information that needs to be protected from unauthorized access or modification.
SHAKEN (Signature-based Handling of Asserted Information Using toKENs)	SHAKEN is an industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network.
SMTP (Simple Mail Transfer Protocol)	SMTP is a protocol used in sending and receiving e-mail.
SOP (Standard Operating Procedure)	SOP is a written directive that provides a guideline for carrying out an activity. The guideline may be made mandatory by including terms such as "shall" rather than "should" or "must" rather than "may."

Term or Abbreviation (Expansion)	Definition / Description
STIR (Secure Telephone Identity Revisited)	STIR is a SIP header-based mechanism for verification that the originator of a SIP session is authorized to use the claimed source telephone number, where session is established with SIP end to end.
VPN (Virtual Private Network)	VPN (Virtual Private Network) is a network implemented on top of another network, and private from it, providing transparent services between networks or devices and networks. VPNs often use some form of cryptographic security to provide this separation. **Relevant NENA Documents:** NENA 75-001, NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
XACML (eXtensible Access Control Markup Language)	XACML (eXtensible Access Control Markup Language) is a general-purpose access control policy language that provides an XML-based syntax for defining rules to control access to resources.

8 References

[1] National Emergency Number Association. "NENA Knowledge Base Glossary." Updated June 16, 2022. https://kb.nena.org/wiki/Category:Glossary.

[2] Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels. S. Bradner*. RFC 2119, March 1997.

[3] National Institute of Standards and Technology. *Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems*. FIPS PUB 199, February 2004.

[4] National Institute of Standards and Technology. *NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations*. Updated December 10, 2020. NIST SP 800-53 Rev 5.

[5] Cybersecurity & Infrastructure Security Agency. "Information and communications Technology Supply Chain Risk Management." Accessed March 17, 2023. https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management.

[6] National Emergency Number Association. NENA i3 Standard for Next Generation 9-1-1. NENA-STA-010.3-2021. Arlington, VA: NENA, approved July 12, 2021.

[7] FOIA Improvement Act of 2016, 5 U.S.C. § 552 (2016).

[8] Access to Information Act, R.S.C. 1985, c. A-1 (Can.).

[9] Privacy Act, R.S.C. 1985, c. P-21 (Can).

[10] Cybersecurity & Infrastructure Security Agency. "Protected Critical Infrastructure Information (PCII) Program." Accessed March 17, 2023. https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program.
[11] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201 (1996).
[12] Cybersecurity & Infrastructure Security Agency. *Cyber Risks to Next Generation 9-1-1*. https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf, November 2019.
[13] National Institute of Standards and Technology. *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments*. NIST SP 800-30 Rev 1, September 17, 2012.
[14] Communications Security, Reliability, and Interoperability Council VII. *Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG9-1-1 Implementations*. https://www.fcc.gov/files/csric7reportsecuirtyrisk-bestpracticesmitigation-legacytransitionalng911pdf, September 16, 2020.
[15] National Institute of Standards and Technology. "Cybersecurity Framework." Accessed March 17, 2023. https://www.nist.gov/cyberframework.
[16] Communications Security, Reliability, and Interoperability Council VII. *Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and Next Generation 9-1-1 (NG9-1-1) Networks*. https://www.fcc.gov/file/20607/download, March 10. 2021.
[17] US-CERT. *Data Backup Options*. P. Ruggiero and M. Heckathorn. https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf, October 2012.
[18] Forum of Incident Response and Security Teams, Inc. *Common Vulnerability Scoring System v3.1: Specification Document*. Updated June 2019. https://www.first.org/cvss/specification-document.
[19] National Institute of Standards and Technology. *NIST Special Publication 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology*. NIST SP 800-40 Rev 4, April 2022.
[20] National Institute of Standards and Technology. *NIST Special Publication 800-92, Guide to Computer Security Log Management*. NIST SP 800-92, September 13, 2006.
[21] National Institute of Standards and Technology. *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*. NIST SP 800-61 Rev 2, August 6, 2012.
[22] National Institute of Standards and Technology. *NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems*. NIST SP 800-34 Rev 1, Updated November 11, 2010.

[23] National Institute of Standards and Technology. *NIST Special Publication 800-184, Guide for Cybersecurity Even Recovery*. NIST SP 800-184, December 22, 2016.
[24] National Institute of Standards and Technology. *NIST Special Publication 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management*. NIST SP 800-63B, Updated March 2, 2020.
[25] National Institute of Standards and Technology. *NIST Special Publication 800-81-2, Secure Domain Name System (DNS) Deployment Guide.* NIST SP 800-81-2 Rev 1, September 18, 2013.
[26] National Institute of Standards and Technology. *NIST Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise*. NIST SP 800-124 Rev 1, June 21, 2013.
[27] National Institute of Standards and Technology. *NIST Special Publication 800-12 Revision 1, An Introduction to Information Security*. NIST SP 800-12 Rev 1, June 22, 2017.
[28] Cybersecurity & Infrastructure Security Agency. "Understanding Denial-of-Service Attacks." https://www.cisa.gov/news-events/news/understanding-denial-service-attacks, February 1, 2021.
[29] Cybersecurity & Infrastructure Security Agency. "Next Generation 911." https://www.cisa.gov/resources-tools/resources/next-generation-911, January 18, 2022.
[30] National Institute of Standards and Technology. *NIST Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy*. NIST SP 800-41 Rev 1, September 28, 2009.
[31] National Institute of Standards and Technology. *NIST Special Publication 800-77 Revision 1, Guide to IPsec VPNs*. NIST SP 800-77 Rev 1, June 26, 2020.
[32] National Institute of Standards and Technology. *NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST SP 800-94, February 15, 2007.
[33] National Institute of Standards and Technology. *NIST Special Publication 800-45 Version 2, Guidelines on Electronic Mail Security*. NIST SP 800-45 Version 2, February 20, 2007.
[34] National Institute of Standards and Technology. *NIST Special Publication 800-175B Revision 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. NIST SP 800-175B Rev 1, March 31, 2020.
[35] NG9-1-1 Interoperability Oversight Commission. *Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy v1.1*. Updated February 22, 2023. https://ng911ioc.org/library/.
[36] NG9-1-1 Interoperability Oversight Commission. *NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines*. Updated February 9, 2022. https://ng911ioc.org/library/.

[37] National Security Agency. *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations*. Updated January 5, 2021. https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF.

[38] National Institute of Standards and Technology. *NIST Special Publication 800-57 Part 2 Revision 1, Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*. NIST SP 800-57 Part 2 Rev 1, May 29, 2019.

[39] National Institute of Standards and Technology. *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitation*. NIST SP 800-88 Rev 1, May 29, 2019.

[40] National Institute of Standards and Technology. *NIST Special Publication 800-207, Zero Trust Architecture*. NIST SP 800-207, August 11, 2020.

9 Appendix A – Zero-Trust Architecture

Zero-trust architecture focuses on protecting resources instead of focusing on the perimeter. It moves away from the "trust but verify" model and into a "trust no one and verify everything" model. It enhances NG9-1-1 network security. Trust is no longer assumed by default for being inside the network. Nothing is trusted automatically. All connections must be authenticated and authorized.

NIST has identified a set of basic tenants that should ideally be fully implemented for zero-trust. These zero-trust basic tenants are the following:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resources authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

Some challenges in implementing zero trust architecture are the following:

- Product support of zero-trust architecture.
- Product interoperability with zero-trust architecture.
- Having strong identity governance.
- Security of the zero-trust controls.
- Ability to recognize attacks and detect malicious activities.
- User impact.
- Internal resistance to change.

For more information, see NIST SP 800-207, *Zero Trust Architecture* [40]

10 Appendix B – Suggested Procurement Security Questions

This section provides a series of security questions that can help determine the security posture of a vendor. This is by no means intended to be a complete list and is provided as a starting point. Not all questions will be relevant to every situation. The answers to these questions can help identify potential security risks and may help with the vendor selection process. "M" is intended as a management control and "T" is intended as a technical control. The questions are broken up into four categories. The category that best fits should be used.

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
1.00	**Organizational Controls**				
1.01	Does the vendor maintain a single point of contact for escalation of security issues?	M	M	M	M
1.02	Does the vendor maintain a security organization capable of incident response?	M	M	M	M
1.03	When contacted, does the vendor give an estimated response time?	M	M	M	M
2.00	**Policy**				
2.01	Does the vendor maintain security policies, applicable to both the organization and the development process?	M		M	M
2.02	Are vendor policies documented and available for access by employees/customers?	M	M	M	M
3.00	**Access Controls**				
3.01	Can it integrate with an enterprise identity management system (e.g., Directory Services)?	T			

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
3.02	Are users prohibited from having multiple concurrent connections (active sessions)?	T		T	
3.03	Are there password controls for timeout, complexity, and reuse?	T		T	
3.04	Are new users forced to change their password upon first login?	T		T	
3.05	Are passwords stored in an encrypted format?	T		T	
3.06	Is multifactor authentication supported?	T		T	
3.07	Are complex passwords enforced?	T		T	
3.08	Are accounts that have gone unused for a specified period of time automatically disabled?	T		T	
3.09	Are inactive users automatically log off?	T		T	
3.10	Is it capable of delegated administration for user provisioning?	T		T	T
3.11	Does it limit access by user role?	T		T	T
3.12	Does it include firewall capabilities?	T	T		
3.13	Is virus & spyware detection and elimination software installed? If not, does/will the software support it?	T	T	T	
3.14	Network Peer Entity Authentication: Do both users and processes identify and authenticate themselves prior to the exchange of data?	T		T	

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
3.15	Does installation documentation specify which OS services need to be enabled for the app to function?	T	T	T	
3.16	If the device is pre-configured, has it been configured with minimal services or to a specific security standard? Is a copy of those standards available?		T		
4.00	**Development Controls**				
4.01	Was it developed using secured platforms with non-default configurations?	M			
4.02	Is a formal development process used that allows the specification of security controls? Is it a commercial process? Which?	M			
4.03	Is security testing and evaluation performed prior to going to production-ready status?	M		M	
4.04	Is a source code review performed for common security coding errors?	M		M	
4.05	Can additional or special security controls be included in future releases?	M		M	
4.06	Is source code distribution limited to vendor developers?	M		M	
4.07	Is source code allowed outside the vendor's facilities during development?	M		M	

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
4.08	Does the vendor conduct security-specific training for coders/developers?	M		M	
4.09	Where is it developed?	M		M	
4.10	Is source code available for escrow and review by customers?	M		M	
5.00	**Physical Controls**				
5.01	Does the vendor software production facility maintain physical controls over ingress/egress?	M		M	M
6.00	**Personnel Controls**				
6.01	Does the vendor perform background checks on employees? Including credit check?	M	M	M	M
6.02	Does the vendor educate employees on security awareness?	M	M	M	M
6.03	Does the vendor require employees to sign a non-disclosure agreement?	M	M	M	M
6.04	Is adherence to security policy a condition of employment at the vendor?	M	M	M	M
7.00	**Continuity and Availability Controls**				
7.01	Is it capable of high-availability configuration?	T	T	T	
7.02	Is it capable of sync/replication to a remote site?	T		T	
7.03	Does it have built-in backup capability?	T		T	

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
8.00	**Operations and Maintenance Controls**				
8.01	With what frequency and on what schedule have security patches been released?	M	M	M	
8.02	Are updates proved as incremental patches or whole replacement software images?	M	M	M	
8.03	Does it support remote access by the vendor? With what methods? Strong authentication required?	M	M		
8.04	Can vendor support activities be mapped back to an individual?	M	M	M	M
8.05	Can remote support be disabled by an operator and enabled only when necessary?	M	M		M
8.06	Does it depend on any external applications, services, or software (DNS, database, SMTP, etc.)	T	T	M	M
8.07	With what frequency are application upgrades released?	M	M	M	
8.08	Does the vendor maintain visibility into security vulnerability data as it applies to it?	M	M	M	M
9.00	**Auditability and Monitoring Controls**				
9.01	Does it log unsuccessful authentication attempts?	T	T	T	

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
9.02	Does it have the capability to "alert"? How?	T	T	T	
9.03	Does it log READ access activity?	T			
9.04	Does it log WRITE access activity?	T			
9.05	Does it log MODIFY access activity?	T			
9.06	Does it self-generate audit reports based on log entries?	T	T	T	
9.07	Does it rotate and archive activity logs?	T	T	T	
9.08	Does it provide the ability to specify maximum log file size?	T	T		
9.09	Can it export audit or log data to an external system for archive and analysis? (syslog, SIM, etc.)	T	T	T	
9.10	Are audit log files protected from unauthorized alteration from system users and/or by the vendor support staff?	T	T	T	
9.11	Does it have the capability to obfuscate or remove specified fields or entries, to protect confidential information?	T		T	T
9.12	Does it track vendor support activities?	T	T	T	T
10.00	**Third-Party Security**				
10.01	Was it developed using resources external to the vendor?	M	M	M	M
10.02	Are vendor third parties contractually obligated to maintain security controls?	M	M	M	M

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
10.03	Are vendor third parties periodically audited for compliance with security obligations?	M	M	M	M
10.04	Do third-party contracts stipulate penalties for noncompliance with security obligations?	M	M	M	M
11.00	**Assurance**				
11.01	Has it been certified with any industry-standard certifications?	M	M	M	M
11.02	Is it capable of digital transaction signatures?	T		T	
11.03	Can it utilize an external certificate authority?	T		T	
11.04	Has it been assessed for security by an objective third party? Results available?	M		M	M
11.05	Does it provide transactional integrity controls?	T		T	
11.06	Does it provide transactional non-repudiation controls?	T		T	
11.07	Are its security features documented for administrators?	M	M	M	M
11.08	Does it use encryption for storage? What algorithms?	T		T	
11.09	Does it use encryption in transit? What algorithms?	T		T	
12.00	**Compliance**				
12.01	Is it compliant with the X.509 certificate standard?	M		M	
12.02	Is it compliant with the PCKS11 key distribution standard?	M		M	

#	Questions	Software or Applications	Physical or Virtual Equipment	Managed Services	Professional Services
12.03	Is it capable of using SAML assertions?	T		T	
12.04	Is it capable of encrypting activity logs?	T		T	
12.05	Does it use standard IANA port assignments?	T			
12.06	Does it lend itself to deployment in a standard 3-tier (presentation, application, data) architecture?	T			
12.07	Is it compliant with required messaging format(s)?	T		T	T

11 Appendix C – Patching

Patching corrects identified security vulnerabilities, functionality flaws, and/or adds new features. This appendix is primarily concerned with fixing identified security vulnerabilities. Once patches for security vulnerabilities are released, malicious actors become aware of the vulnerability and may attempt to exploit unpatched systems. Therefore, it is imperative that patches be applied as soon as it is safely feasible. If unable to apply a released patch, appropriate mitigation steps should be taken to help protect against exploitation of the vulnerability until the patch can safely be applied.

Care must be taken when applying patches. Patches may break other applications or cause a disruption in a NG9-1-1 system. Some patches require operating system reboots or may require application restarts. Either of which may cause unanticipated downtime. Therefore, care must be taken when applying patches, especially to mission critical systems. Patches should be tested before applying and rolled out in a controlled manner so that all systems are not affected at the same time.

Patch management best practices are to:

- Have a complete and updated inventory of the entire NG9-1-1 system. The first step in patch management is knowing what you have. This is accomplished by obtaining an up-to-date inventory of all hardware, software, firmware, and installed patches within a NG9-1-1 system to include version numbers and installed patches were applicable. This inventory will allow for easy determination of what needs to be patched and what has been patched. It is highly recommended that this inventory be accomplished using an automated application capable of periodically querying all hardware and software for the required information and presenting that information as needed.
- Group systems based on criticality and business function. These groups should then be further subdivided into two or more subgroups to facilitate structured patch rollouts. Patches should then be pushed out to the initial test subgroups for each group and allowed to burn in for a predefined period of time before rolling them out to the rest of the subgroups. This allows for verification that a patch does not have any unforeseen impacts before being rolled out to the entire NG9-1-1 system.
- Routinely check for available patches for each NG9-1-1 system component. This check should be done daily or, at a minimum, in accordance with each manufacturer's patch release cycle. Occasionally patches may be released out of cycle if deemed necessary by the manufacturer. It is recommended that this process be automated.
- Test patches before applying them to the entire NG9-1-1 system. Patches can have unforeseen consequences or could disrupt business functionality. Patches may require a restart of the operating system or an application. Patches may break dependencies. It is imperative to test patches before applying them to check for

issues. Ideally you want to use a test environment first and then roll the patch out to a limited number of test users/systems to validate before rolling the patch out to the entire NG9-1-1 system.

- Establish patching procedures. This procedure needs to cover the approval process, testing process, roll out process, roll back process, and escalation process for patches. These processes may vary depending on severity and/or type of patch.
- Automate patching. A NG9-1-1 system can have many hardware and software components and patching them manually can be very resource intensive. Implementing an automated patching approach helps to greatly decrease workload and ensure a smoother and efficient patch rollout. Many automated patching applications will provide reports on the patching level of all devices and software in its database.
- Periodically conduct vulnerability scans that include checks for missing patches. Many vulnerability scanners check for missing patches and can be used to validate patch levels identified on the inventory. Mostly this will be operating system patches, but additional devices and software detection may be possible depending on the capabilities of the vulnerability scanner used. Like with anti-virus scanners, vulnerability scanners need to be regularly updated. It is recommended that a vulnerability scan be run at least monthly.

For more information on patch management please see NIST SP 800-40, *Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology* [19].

12 Appendix D – Index of Normative Requirements

Note: the section numbers in this Appendix are links to the associated sections above. See those sections for details about each of these summarized normative requirements.

3 Technical Description

3.2 Statement of Compliance

- Non-compliance with security requirements, standards, procedures, and practices SHALL be documented to identify security vulnerabilities, determine associated criticality, and establish a compliance action plan and/or risk acceptance.
- Unresolved non-compliance SHALL require documented risk acceptance as described in Section 4.3 Risk Management.

3.3 Severity Categories

- A cybersecurity audit SHALL follow, at a minimum, the severity categories as defined in NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* [3].

3.4 Roles & Responsibilities

- Every individual within a NG9-1-1 Entity SHALL be informed of their on their respective roles and responsibilities as they apply to NG9-1-1 and included in the security 'mindset' of that Entity, and it SHALL be documented.
- The following responsibilities SHALL be fulfilled:
    - **Security Manager:** Executive or other department manager with the authority and responsible for the security of the Entity. This individual, or their designated representative, SHALL define security policy as it relates to all components, physical and/or digital, of a NG9-1-1 Entity as a whole.
    - **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, declassifying, and disposing of data for which they are the Data Owner for on a NG9-1-1 system. All data, local or remote, in a NG9-1-1 system SHALL have a Data Owner. It does not need to be the same individual for all data. Each Data Owner is responsible for helping a NG9-1-1 Entity understand the importance of the data they are responsible for in order to establish the necessary level of protection.
    - **Data Custodian:** Responsible for ensuring that all security measures required for data, or subset of data, are implemented, adhered to, and maintained. All data, local or remote, at rest and in transit, in a NG9-1-1 system SHALL have a Data Custodian. It does not need to be the same individual for all data.

- **Data User:** Responsible for complying with all security policies and procedures for NG9-1-1 data. Any authorized individual who accesses NG9-1-1 data is a Data User. For example, a Dispatcher is a Data User in that they 'use' 9-1-1 call data to perform their daily tasks.
- **Security Audit Manager:** Responsible for ensuring that periodic audits of a NG9-1-1 system are completed, and all findings are addressed. Audits may be performed by internal or external resources. A risk assessment form SHOULD be conducted for all findings.

4 Policy Management Domain

- The contract SHALL clearly detail the roles and responsibilities of each party and SHOULD include applicable security reviews, assessments, and/or audits to ensure the protection of all relevant information, systems, services, or other resources. Some roles and responsibilities include, but are not limited to, administration, maintenance, patching, management, and recovery.
- When outsourcing data or systems that contain data, the contract SHALL clearly define who owns that data.
- Contractors, suppliers, and subcontractors SHALL protect that data in accordance with the terms and conditions of applicable contractual agreements between the contractor or supplier and a NG9-1-1 Entity.
- In addition, it SHALL be the responsibility of all contractors, suppliers, and subcontractors to comply with applicable federal, state/province/territory, and local acts, statutes, and regulations that relate to the control and authorized use of information and information resources.

4.1 Security Governance

4.1.1 Senior Management

- Senior management SHALL create and model a culture of security as outlined in this document.
- The Senior Management SHALL, at a minimum:
  - Provide documentation defining the security goals and objectives for a NG9-1-1 Entity.
  - Provide the necessary resources to accomplish the security goals and objectives for a NG9-1-1 Entity.
  - Assign the roles and responsibilities for a NG9-1-1 Entity.
  - Retains overall responsibility for a NG9-1-1 Entities security program.
  - Instill and model a NG9-1-1 Entity wide security mind set.

4.1.2 Policies

A NG9-1-1 Entity SHALL, at a minimum, have the following policies:

- **Acceptable Use Policy:** This policy defines what users may or may not do on or with NG9-1-1 system equipment, software, and applications.

- **Auditing and Assessment Policy:** This policy defines the frequency and scope of security audits and assessments.
- **Authentication/Password Policy:** This policy defines authentication and password requirements for a NG9-1-1 Entity.
- **Change Management Policy:** This policy defines the process by which changes can be made to a NG9-1-1 system. This policy defines the documentation and authorization requirements for planned and unplanned changes. It also defines what routine changes are authorized along with any requirements for them.
- **Data Protection Policy:** This policy defines the data classification levels, how that data is to be labeled, handled, stored, managed, and disposed of. The policy will define how third-party data will be handled and will cover public records requests.
- **Equipment Disposal Policy:** This policy defines how equipment will be disposed of.
- **Endpoint Protection Policy:** This policy defines the security controls and patch management for each type of device.
- **Hiring Practices Policy:** This policy defines how employees will be vetted and trained. Their training needs to cover security policies and inclusion in the Security Awareness program.
- **Physical Security Policy:** This policy defines physical access and theft prevention requirements.
- **Procurement Policy:** This policy defines how technical items are purchased in relation to identifying and mitigating security risks (e.g., supply chains, software, hardware) while complying with internal security guidelines and requirements [5].
- **Remote Access Policies:** This policy defines authorized methods for all external remote connections to NG9-1-1.
- **Risk Management Policy:** This policy defines how risk is assessed resulting from threats to the confidentiality, integrity, and availability of NG9-1-1 assets.
- **Security Awareness Training Policy:** This policy defines the frequency and core topics of the Entities security awareness training.
- **Cybersecurity Incident Response Policy:** This policy defines actions and procedures to take in the event of a cybersecurity incident as well as how and when to bring in outside assistance.
- **Security Monitoring Policy:** This policy defines logging, endpoint monitoring, and traffic monitoring and how often that information will be reviewed.

4.1.3 Procedures

- A Standard Operating Procedure (SOP) that details the technology and tasks related to maintaining a secure environment for a NG9-1-1 Entity SHALL be established.
- SOPs SHALL be developed, maintained, periodically updated, and utilized for all identified tasks.

4.1.4 Information Classification and Protection

4.1.4.3 Data Owner

The Data Owner SHALL:

- Assess the risk associated with the loss of data for which they are the Data Owner.
- Judge the value of the data and assign the proper classification level according to the Data Protection Policy.
- Periodically review the classification level for all data for which they are the Data Owner to determine if the status should be changed.
- Communicate access and control requirements to the Data Custodian and users.
- Authorize appropriate level of access using the principle of least privilege for those individuals who have a demonstrated business need for access (read/write/delete).
- Ensure that the required security controls are in place to mitigate the risk to data integrity, confidentiality, and availability.
- Conduct, at a minimum, an annual audit of all data for which they are the Data Owner.
- Monitor safeguard requirements to ensure that information is being adequately protected.

4.1.4.4 Data Custodian

- When an employee, vendor, contractor, agent, or service provider retains data, they SHALL become a custodian for that data.
- A Data Custodian SHALL:
    - Ensure data is used as authorized and only for the purpose intended.
    - Ensure access by authorized users with a demonstrated business need.
    - Maintain the integrity, confidentiality, and availability of the data for which they are the Data Custodian.
    - Comply with information classification and protection policies on retention and disposal of records and data.
    - Ensure required safeguards are being used for processing equipment, information storage, backup, and recovery.
    - Ensure the data is used in an authorized secure processing environment that can adequately protect the integrity, confidentiality, and availability of information.
    - Periodically review data access to ensure that it is only authorized users have access and it is being used for the purpose intended.

4.2 Security Posture Design

4.2.1 Security Assessment Documentation

- All components of a NG9-1-1 system SHALL be covered by a documented security assessment. If desired, a security assessment can cover multiple components rather than an assessment for each individual component.

4.2.2 Information Classification Guidelines

4.2.2.1 Classification Levels

- The Data Protection Policy SHALL specify the different classification levels of data for the Entity.
- The Data Protection Policy SHALL define which classifications levels the Entity believes are not subject to the Freedom of Information Act (FOIA) [7] or similar laws [8][9].
- All data SHALL be assigned a classification level according to the highest sensitivity of any information in that data set.
- 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 a 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.
- Access to sensitive information SHALL be reviewed at least annually.

4.2.2.1.2 Sensitive (Internal Use Only)

- Release of Sensitive (Internal Use Only) Data/information SHALL be documented when released.

4.2.2.1.3 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.

4.2.2.1.4 Sensitive (Most Sensitive Information)

- Most Sensitive Information SHALL only be shared 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.

4.2.2.3 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.

4.2.2.4 Receipt of Sensitive Information

- External party Sensitive Data[6] SHALL be safeguarded in the same manner as like data for the Entity and classified as such.

4.2.2.5 Protecting Sensitive Information

- To protect NG9-1-1 Entity data, policies SHALL define how each classification level of data is to be handled and protected relevant to the three states of data defined below.

4.2.2.5.1 Data at Rest (Stored Data)

- Personally owned storage devices (i.e., user owned USB thumb drives, memory card, phones) SHALL **NOT** be used. Entity-owned and approved storage devices such as USB thumb drives, memory cards, CDs/DVDs, MAY be used based on the NG9-1-1 Entity's Data Protection Policy.
- Protection of Sensitive Data at rest SHALL be defined in the Data Protection Policy.
- The integrity of data at rest SHALL be maintained in a manner that assures that no unauthorized modifications or changes are made to the data.
- Disk encryption (full/partial) for Sensitive Data SHALL be defined in the Data Protection Policy. Storing Sensitive Data on CDs/DVDs should be avoided.
- Destruction and/or disposal procedures for Data SHALL be defined in the Disposal Policy.

4.2.2.5.2 Data in Transit (or in motion)

- Sensitive Data requires encryption as defined in NENA-STA-010.3 [6] and SHALL be defined in the Data Protection Policy.

4.2.2.5.3 Data in Use

- Data in use SHALL be safeguarded from unauthorized disclosure.
- The protection of Sensitive Data SHALL be defined in the Data Protection Policy. Additional sections for the protection of data may be included in the Data Protection Policy or separate policies such as a Clean Desk policy and Print Policy.
- NG9-1-1 Entity personnel SHALL ensure that re-used storage media is "clean" (i.e., it does not contain a residual of information from previous uses).

[6] Sensitive Data is information that needs to be protected from unauthorized access or modification.

- All media distributed outside NG9-1-1 Entity SHALL be new or come directly from a recognized pool of "clean" media.

4.2.2.6 Safeguarding Sensitive Electronic Information

Where data marked Sensitive (Internal Use Only), Sensitive (Restricted), and Sensitive (Most Sensitive Information) is stored on removable or portable media (such as USB flash drives, thumb drives, memory sticks, external hard drives, or CDs), and/or mobile computing devices, 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).
- SHALL be kept in the direct supervision of the custodian when traveling on public transport (e.g., not be placed in taxi trunk/boot, bus hold/baggage storage, checked-in on airplane).

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

- In NG9-1-1 systems, the encryption algorithm SHALL be AES 256.

Mobile computing devices containing Sensitive Data (Most Sensitive Information) SHOULD **NOT** be taken outside the NG9-1-1 Entity controlled space, but if there is an overriding business need to do so then:

- Approval SHALL be documented in writing.
- Exceptions to the policy SHALL be documented in writing.
- Whenever systems containing sensitive information require repair, the repair SHALL use only authorized technicians, approved repair processes, the work done at an approved location, and the system secured in accordance with applicable non-disclosure agreements, laws, regulations, and policies to ensure that information contained on the devices is safeguarded.

4.2.2.7 Safeguarding Sensitive Electronic Information in the Cloud

Where Sensitive (Internal Use Only), Sensitive (Restricted), and Sensitive (Most Sensitive Information) data (such as private keys, credentials, passwords, certificates) is stored in the cloud it:

- SHALL use cloud vendor provided mechanisms such as Private Key protection and management methods (Key Vaults, Key Management Systems, etc.). For very high assurance security cases, NG9-1-1 entities SHOULD protect Private Keys with Hardware Security Modules (HSM).

The cloud vendor provided mechanisms used by NG9-1-1 entities:

- SHALL support audit logging, monitoring, access control and data encryption when Services are offered as Software as a Service model (SaaS).

- SHOULD adhere to broadly accepted security conventions, e.g., NIST-800, CIS Controls, or other locally applicable controls.

4.2.3 Transport and Shipping of Electronic Media and Devices

- Media or devices containing Sensitive (Most Sensitive Information) SHALL be hand delivered by the Data 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.

4.2.4 Safeguarding Printed Information/Material

4.2.4.1 Sensitive (Internal Use Only) – Printed Material

- Inside Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from visitors who have no need to see the information.
  - Observe sending and receiving fax machines with authorized personnel or use fax machines in offices/areas where access is limited to authorized personnel.
  - Ensure that Printed Material is shredded when no longer needed.
- Outside Controlled Space user(s) SHALL:
  - Ensure Printed Material is secured from unauthorized access.
  - Ensure Printed Material is kept in the direct supervision of the custodian.
  - Ensure Printed Material is in direct supervision of the Data Custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).
  - Observe the printer or copier with an authorized person for the information.
  - 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.
  - Supervise fax machines that are located outside the controlled space with authorized personnel.
  - Ensure Printed Material is shredded when no longer needed.

4.2.4.2 Sensitive (Restricted) – Printed Material

- Inside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from casual observers.
  - Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe). However, if the controlled space is only accessible to authorized individuals, it is not necessary to keep hidden or physically secured when unattended.

- Monitor the printer or copier unless printer/copier is in an office/area where access is limited to authorized personnel.
- Ensure Printed Material is hand delivered by originator or Data Custodian.
- Use double envelopes with the inner envelope marked "Private" when using internal mail.
- Supervise sending and receiving fax machines with authorized personnel or use fax machines in offices/areas where access is limited to authorized personnel.
- Ensure Printed Material is shredded when no longer needed.

- Outside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from casual observers.
  - Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
  - Ensure Printed Material is in direct supervision of the Data Custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).
  - Monitor the printer or copier with a person authorized for the information.
  - 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.
  - Monitor fax machines that are located outside NG9-1-1 Entity controlled space with authorized personnel.
  - Ensure Printed Material is shredded when no longer needed.

4.2.4.3 Sensitive (Most Sensitive Information) – Printed Material

- Inside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is kept away from casual observers.
  - Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe).
  - Monitor the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.
  - Ensure Printed Material is hand delivered by the originator or Data Custodian.
  - Ensure Printed Material is not faxed.
  - Ensure Printed Material is shredded when no longer needed.

- Outside the Controlled Space user(s) SHALL:
  - Ensure Printed Material is never taken outside the controlled space.
  - **However, if there is an overriding business need to take Printed Material outside the controlled space, then:**
    - Obtain approval from a Senior Manager.

- Kept away from casual observers.
- Kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).
- Stay in direct supervision of the custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).
- Monitor any print/copy outside the controlled space.
- Hand delivered by the data owner or data custodian.
- Not be faxed.
- Ensure Printed Material is shredded when no longer needed.

4.2.5 Disclosure of Information

- The Data Protection Policy SHALL define what data can be placed in the public domain and what data is exempt from public disclosure.
- The Data Protection Policy SHALL define who may request what types of data and how those requests are to be made. A possible example of this would be limiting 9-1-1 call records to the individual making the call, law enforcement, and/or court orders. Refer to local laws and regulations for further guidance.
- Documentation for public records requests SHALL be maintained in accordance with the 9-1-1 Entities retention requirements. These documents will contain, at a minimum, who requested the data, when it was provided, and what was provided.

4.3 Risk Management

- A NG9-1-1 Entity SHALL have a documented Risk Management process that, at a minimum, evaluates vulnerabilities, threats, and risks.
- A NG9-1-1 Entity SHALL have a documented risk acceptance form.
- There SHALL be a risk acceptance form covering every identified risk the entity has direct control over.
- Each risk acceptance form SHALL be signed off by a senior level manager within a NG9-1-1 Entity with the authority to accept the risk on behalf of a NG9-1-1 Entity.
- A NG9-1-1 Entity SHALL annually, at a minimum, reassess all risk management forms. Critical and high-level risks SHOULD be reviewed and reassessed at least monthly.

4.3.1 Threat Vectors

- The PSAP and authority having jurisdiction SHALL ensure that Service Level Agreement(s) (SLA) addresses all threat vectors.

4.4 Change Management

- All changes to equipment and/or configuration of a NG9-1-1 system SHALL be reviewed and approved in accordance with the Change Management policy.
- All changes to equipment and/or configuration of a NG9-1-1 system SHALL include a documented security review.

- All changes SHALL be documented. This may consist of new documentation for new equipment or updates to existing documents for configuration changes.

Note: For unplanned changes, any of the SHALL statements above may need to be completed after the change.

5 Operations Management Domain

5.1 Cybersecurity Training

5.1.1 Cybersecurity Awareness Training

- All users of a NG9-1-1 system SHALL be trained 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 users of a NG9-1-1 system SHALL, at a minimum, complete Cybersecurity Awareness Training annually. This training will include instruction on how to recognize potential threats that a user could reasonably expect to encounter. Cybersecurity Awareness Training must also use parts of the Cybersecurity Incident Response Plan, which includes the notification and escalation process for users, the primary points of contact, and the process for submitting a cybersecurity event.

5.1.2 Technician Security Training

- Entities responsible for system and/or security administration (including those contracted to do such tasks) SHALL employ individuals who have received current security training in their assigned area of responsibility. Security operations, administration, and maintenance training applies to any individual responsible for securing and/or working on any part of a NG9-1-1 system. A NG9-1-1 Entity can require a service provider to supply validation and assurances of a technician's knowledge and skill to perform a task.

5.2 Security Assessments

- A security assessment SHALL be conducted, at a minimum, annually. This may be an internal or external assessment.
- An external assessment SHALL be done, at a minimum, once every 3 years. This SHOULD be done by a different firm/organization than what was used the previously.
- An external assessment, to include gap analysis, SHALL be documented and provided to a NG9-1-1 Security Manager or their designated representative.
- All findings from a security assessment SHALL be addressed. If unable to address the finding fully, a NG9-1-1 Entity must accept any residual risk.
- Security assessments SHALL be retained for a minimum of five years and in accordance with local retention policies. If all parts of an audit no longer cover any

area of the current NG9-1-1 system, it may be disposed of earlier if allowed by local retention policies.

5.4 Inventory

An inventory SHALL, at a minimum, document and track the following:

- Devices
  - Device name
  - Identification (make, model, and serial number)
  - End of life date
  - Firmware version(s) (a device may have multiple components with firmware)
  - Primary location
  - Primary owner/responsible party
  - Highest classification level of data used on/by device
  - Contract/warranty
- Software and applications
  - Software/application name
  - Software/application version
  - Number of licenses
  - End of life date
  - Device(s) installed on
  - Highest classification level of data used on/by software/application
  - Contract/warranty
- Data (by group)
  - Classification level
  - Storage location
  - Data Owner
  - Data Custodian
- Cloud/third-party services
  - Provider
  - Contact info
  - Service provided (i.e., data storage, CPE, e-mail, connectivity)
  - Contract end date
  - Entity administrator/point of contact
  - Highest classification level of data on or used by service
  - Contract/warranty
- Software libraries
  - Path
  - Manufacturer
  - Version number

5.5 Patching and Updating

Note that timely patching is also an effective protection against Brute Force attacks.

- A NG9-1-1 Entity SHALL validate all necessary patches are installed at least monthly.
- Once a mitigation control or patch has been approved through the change management process, and has undergone appropriate testing, it SHALL be applied as soon as possible.
- After a patch or mitigation control is applied to fix a vulnerability, a NG9-1-1 Entity SHALL verify that there is no evidence that the vulnerability was exploited in a NG9-1-1 system.
- A NG9-1-1 Entity SHALL establish timelines for patching CVSSs based on criticality. It is recommended that critical CVSS be patched within 48 hours or less of disclosure.

5.6 Continuous Monitoring

5.6.1 Time Synchronization's Relationship to Continuous Monitoring

- Time synchronization SHALL be in accordance with the Time Server specifications in NENA-STA-010.3 [6].

5.6.2 Security Event Logging

Each NG9-1-1 Entity SHALL:

- Have all logging applications and device clocks synchronized with the time server specified in Section 5.6.1 Time Synchronization's Relationship to Continuous Monitoring. This allows logs to be easily correlated between different devices and applications through their timestamps.
- Have sufficient logging to be able to trace and correlate events throughout a NG9-1-1 Entities' system. This may require additional logging requirements for administrative accounts. See note below.
- Review logs at least weekly by an individual. This should be done more frequently with the ideal being as close to real time as possible. To achieve this, automation will be required. The NG9-1-1 Logging Service includes standardized log retrieval functions that can assist such automation. See Section 5.6.3 Information and Event Management.
- Protect logs from unauthorized deletion or modification.
- Retain logs in accordance with local retention requirements.

5.6.4 Intrusion Monitoring and Detection

- There SHALL be a defined process or procedure identifying when and how often the periodic review of security monitoring systems will be done.

5.6.5 Incident Detection and Response

- A NG9-1-1 Entity SHALL have a Cybersecurity Incident Response plan.

5.7 Recovery Operations

- A NG9-1-1 Entity SHALL have the following recovery plans. They may be separate or combined. It is recommended that they are separate plans.
  - Business Continuity plan
  - Disaster Recovery plan
  - Cybersecurity Incident Response plan
- These plans SHALL be maintained offline and be accessible to recovery teams.
- These plans SHALL be reviewed at least annually and updated as needed.

5.7.1 Forensics

- A NG9-1-1 Entity SHALL have documented procedures outlining what forensic evidence should be captured and preserved.
- A NG9-1-1 Entity SHALL have documented procedures outlining how forensic evidence should be captured.
- A NG9-1-1 Entity SHALL have documented procedures outlining how to establish and maintain chain of custody of forensic evidence in accordance with local governance.

5.7.2 System Backup and Restoration

5.7.2.2 Validating and Testing Backups

- A NG9-1-1 Entity SHALL have a documented backup plan.
- A NG9-1-1 Entity SHALL have documented recovery procedures.
- A NG9-1-1 Entity SHALL test their backup plan annually at a minimum.

6 Security and Risk Management Domain

6.1 Perimeter Security

- All NG9-1-1 Entity information resources SHALL be kept physically secured and protected from theft, misappropriation, misuse, unauthorized access, and damage.
- A controlled area entry and exit log SHALL be maintained for every controlled area.
- Physical access control devices/keys issued to an individual SHALL never be loaned or shared with another individual.
- A person possessing an access control device/key SHALL never use that device/key to allow access to an unauthorized individual.

6.1.1 Physical Protections

- NG9-1-1 facilities SHALL have adequate perimeter access control. These may include fencing, video cameras, lighting, guarded access points, etc.
- The perimeter of a physically secure location SHALL be prominently posted and separated from non-secure locations by physical controls.
- All entry points to secured locations SHALL be prominently marked.

6.1.2 Physical Access Authorizations

- A NG9-1-1 Entity SHALL develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or SHALL issue credentials to authorized personnel.
- Non-NG9-1-1 Entity employees who are issued any devices and/or keys that grant access to NG9-1-1 Entity facilities SHALL be sponsored by a NG9-1-1 Entity management individual.
- Documentation on sponsorship and results of all local, state, and federal guidelines (i.e., background checks) SHALL be maintained for each non-NG9-1-1 Entity employee who is granted access.
- Non-NG9-1-1 Entity employee documentation SHALL be retained for a duration defined by the local retention policy.

6.1.3 Physical Access Control

- A NG9-1-1 Entity SHALL control all physical access points (except for those areas within the facility officially designated as publicly accessible) and SHALL verify individual access authorizations before granting access.
- Everyone entering a controlled access facility SHALL follow the physical access control procedures in place for that facility.
- A controlled area entry and exit log SHALL be maintained of everyone entering and exiting a controlled area.
- Controlled area entry and exit log files SHALL be retained for a duration defined by the local retention policy.
- 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. Measures SHOULD be in place to prevent tailgating.
- Doors to controlled access areas SHALL **NOT** be propped open.
- Everyone in a controlled area SHALL be vigilant while inside and challenge and/or report unidentified persons including persons not displaying identification badges (for more on display badges see Section 6.1.7 Identification Badges.
- Physical access control devices/keys issued to an individual SHALL never be loaned or shared with another individual.
- A person possessing an access control device/key SHALL never use that device/key to allow access to an unauthorized individual.

6.1.4 Access Control for Transmission Medium

- A NG9-1-1 entity SHALL control physical access to information system distribution and transmission lines within a physically secure location.

6.1.5 Access Control for Display Medium

- A NG9-1-1 Entity SHALL control physical access to information system devices.
- A NG9-1-1 Entity SHALL position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing.

6.1.6 Monitoring Physical Access

- A NG9-1-1 Entity SHALL monitor physical access to the information system to detect and respond to physical security incidents.

6.1.7 Identification Badges

- NG9-1-1 Entity employees, authorized non NG9-1-1 employees, and visitors SHALL be issued an identification badge.
- Employee and authorized non-employee's identification badges SHALL display a picture of the individual the card was issued to.
- The issuance of temporary badges for authorized employees who do not have their official badge SHALL follow local policy and procedures.
- The issuance of a visitor badge SHALL follow local policy and procedures.
- Individuals with visitor badges SHALL be escorted while within non-public areas.
- Visitor and temporary badges SHALL be easily and clearly identifiable.
- Identification badges SHALL be prominently displayed while within NG9-1-1 Entity premises.
- If entry points are staffed, identification badges SHALL be presented to the individual at the entry point prior to being allowed in.
- Individuals who do not have an authorized badge or are unwilling to show their badge SHALL be escorted off the premises in accordance with local policy and procedures.
- Visitor and temporary badges SHALL be turned in when leaving a NG9-1-1 facility.
- Lost or stolen badges SHALL be reported as soon as discovered and any access the badge may have allowed disabled within 24 hours of notification.

6.1.8 Visitor Control

- A NG9-1-1 Entity SHALL control physical access by authenticating visitors before authorizing escorted access to any physically secure location (except for those areas designated as publicly accessible).
- The NG9-1-1 Entity SHALL always escort visitors and monitor visitor activity.

6.1.9 Delivery and Removal

- A NG9-1-1 Entity SHALL authorize and control information system-related items entering and exiting the physically secure location.

6.2 Access Control

- Each user SHALL have a unique account.

- All guest and/or anonymous accounts SHALL be disabled.
- Role-based access controls SHALL be used.
- Role-based access controls SHALL be reviewed at least annually.

6.2.1 Account Management

- Creation or modification of accounts SHALL be approved by an authorized representative of a NG9-1-1 Entity.
- Requests for the creation of and/or modification to accounts SHALL be made through an established process that is documented and audited.
- Individuals administrating accounts SHALL ensure that only approved creation or changes to accounts are made.
- The identity of users requesting password resets SHALL be validated before providing any password reset services.

6.2.1.1 Account Change

- The user's manager SHALL, within one working day, notify account manager(s)/administrator(s) of the change.
- The account manager(s)/administrator(s) SHALL, within one working day of notification, remove access to unauthorized resources and information from the user's account.
- For terminated user accounts or accounts that are no longer needed, the account manager(s)/administrator(s) SHALL, within one working day of notification, disable the user account. The account SHOULD be deleted in accordance with a NG9-1-1 Entity's procedures.
- For a user's account still working for a NG9-1-1 Entity, the user's manager SHALL obtain approval for new access needs from the authorized representative and provide that documentation to the account manager(s)/administrator(s) as soon as possible.
- The account manager(s)/administrator(s) SHALL, within one working day of receipt of the authorization documentation, provide the approved access for the user's account.
- All accounts SHALL be reviewed at least annually for authorized privileges and access.
- Any changes SHALL be reported to the account manager(s)/administrator(s) by an authorized representative.
- Any identified changes SHALL be completed by the account manager(s)/administrator(s) within one working day.

6.2.1.2 All Accounts

- All accounts SHALL have a valid business need.
- All accounts SHALL be approved by an authorized representative.
- All accounts SHALL be checked at least monthly for inactivity.

- All accounts SHALL be reviewed at least annually.
- Unused accounts SHALL be disabled and deleted in accordance with a NG9-1-1 Entity's procedures.
- All accounts SHALL have a unique password that conforms with the Authentication/Password policy.
- All account passwords SHALL be changed in accordance with the Authentication/Password policy.
- Accounts with temporary passwords SHALL require a password change upon first login with the account.

6.2.1.3 Administrator Accounts

- Administrator permissions SHALL only be granted to authorized individuals with a valid business need.
- Administrator accounts SHALL only be used to conduct official NG9-1-1 activities.
- Administrator accounts SHALL **NOT** be used for day-to-day user level activities.
- Administrator accounts SHALL only be used to perform an authorized activity requiring elevated permission.
- Local administrator accounts SHALL **NOT** be used when individual domain administrator accounts are an option.
- Non-unique local and domain administrator accounts (i.e., default admin accounts) SHALL only be used during initial installation or under disaster recovery scenarios.

6.2.1.5 Service Accounts

- A service account SHALL **NOT** be used as a user account.
- A user or administrator account SHALL **NOT** be used as a service account.
- Each service account SHALL be documented sufficiently to identify what it is used for and where it is used.
- A service account SHALL only have the required permissions and access required to perform the action for which it was made (least privilege).
- Each service account SHALL be dedicated to a single service.
- Service accounts SHALL be prevented from interactive login unless there is a specific business need.

6.2.1.6 Guest / Temporary Accounts

- Guest and Anonymous accounts on NG9-1-1 networks and systems SHALL be disabled.

6.2.2 Default Credentials and Control of Authentication Credentials

- New devices and applications that have local accounts SHALL have a new password set in accordance with the Authentication/Password policy for each local account prior to being connected to any system/network.

6.2.3 Login

- Access to all systems from external or remote connections SHALL utilize multi-factor login authentication.
- All users of a NG9-1-1 system SHALL be required to authenticate before being allowed access.
- User passwords SHALL **NOT** be visibly displayed when entered.
- Failed authentications SHALL **NOT** identify the reason for the failure.
- After no more than five failed attempts, the user account SHALL be locked out for at least 10 minutes or based on local access policy. An authorized individual may be permitted to unlock an account sooner than 10 minutes if necessary.
- Passwords SHALL **NOT** be hard coded into login sequences or scripts.

6.2.4 Logon Banners

- NG9-1-1 Entity SHALL develop legally acceptable banner messages.
- NG9-1-1 Entity devices SHALL display a banner message during the log in sequence.
- The banner SHALL require active acceptance prior to completing the login process and gaining access to any resources or data. Active acceptance requires input from the user.

6.2.5 Passwords/Passphrases

- Users SHALL **NOT** use their Passwords/Passphrases for any other account they may have.
- Passwords/Passphrases SHALL consist of 16 or more characters.
- Passphrases SHALL consist of a minimum of three different words or word segments. These should be words that do not typically go together.
- A Passwords/Passphrases SHALL consist of upper-case letters, lower-case letters, numbers, and symbols.
- Passwords/Passphrases SHALL **NOT** consist of sequential characters or words that repeat three or more times.
- Passwords/Passphrases SHALL be changed if they are expected to have been compromised.

6.2.6 Password Manager

- Only password managers approved by the Security Manager SHALL be used.
- Multi-factor authentication SHALL be required to gain access to any password manager.
- A user's password manager SHALL **NOT** be shared with another user.
- Users SHALL report the loss or suspected compromise of a password manager within one working day of discovery.
- All passwords stored on a lost or potentially compromised password manager, or password manager's database, SHALL be changed within one working day of discovery.

6.3 Device Connectivity

- A NG9-1-1 Entity SHALL maintain current documentation on all connections to their NG9 1-1 system.
- All connections transporting sensitive information SHALL be secured (e.g., CJIS, HR, NGCS, CHFE).

6.3.1 Multi-Homed Host

- If there is a valid business requirement for a host to be multi-homed, the implementation SHALL be approved, documented, have adequate security measures in place, have appropriate logging, and be monitored. Adequate security measures would entail security controls like anti-virus, host firewall, IDS/IPS, etc. Logging is covered in Section 5.6.2 Security Event Logging above.

6.3.2 Wi-Fi

If a NG9-1-1 Entity decides to implement Wi-Fi then they SHALL, at a minimum, take the following actions:

- Change default password(s) in accordance with the Authentication/Password Policy.
- Change the SSID(s) from the default to one that is not easily associated with the device or a NG9-1-1 Entity (consider hiding non-public SSIDs).
- Disable device management over Wi-Fi.
- Use WPA2-PSK-AES (current standard as of this writing) or stronger standard with a strong password in accordance with the Authentication/Password Policy.
- Use a different SSID and WPA2 password if using a Guest network, and ensure it cannot connect to (air gapped from) a NG9-1-1 network.

6.3.3 Other Wireless

- NG9-1-1 Entities SHALL ensure that devices that contain or process sensitive information are prevented from transmitting that information through any of these unsecured technologies.

6.3.4 Broadband Cellular

- If a NG9-1-1 Entity incorporates broadband cellular they SHALL ensure the connection has appropriate security.

6.3.5 Peer-to-Peer

- P2P SHALL only be allowed for those programs or applications that cannot achieve their legitimate business purpose or mission in any other way.
- If P2P is allowed, a NG9-1-1 Entity SHALL ensure there is a control in place to validate and verify the information.
- If P2P is allowed, a NG9-1-1 Entity SHALL limit the P2P sharing to a NG9-1-1 domain.

6.4 Domain Naming System (DNS)

- NG9-1-1 Entities SHALL enable DNSSEC on all network DNS servers.
- NG9-1-1 Entity clients SHALL request DNSSEC validation.
- NG9-1-1 Entity zone transfers SHALL be restricted to only authorized servers. This SHOULD be accomplished through access control lists.
- NG9-1-1 Entity DNS servers SHALL have DNS logging enabled.
- NG9-1-1 Entity DNS servers SHALL have the DNS cache locked and set to 100% of time to live.
- NG9-1-1 Entity DNS name servers SHALL have response time limits set.
- Primary DNS servers SHALL **NOT** be publicly accessible.
- Only authorized administrators SHALL have access to primary DNS servers. This SHOULD be accomplished through access control lists.
- Publicly accessible DNS servers SHALL be authoritative-only.
- All accounts with privileged access to DNS SHALL follow administrative account requirements. See Section 6.2.1.3 Administrator Accounts.
- All NG9-1-1 Entity DNS servers SHALL follow patching and updating requirements. See Section 5.5 Patching and Updating.

6.5 Rights & Privileges

- Access to data SHALL be limited only to those whose roles require access.
- Privileged access to Sensitive Data SHALL only be given to those with a valid need to know.
- Users SHALL only be given the minimum permissions necessary to perform their job, also known as the principle of least privilege.
- Role based access SHALL be used to assign rights and privileges and SHALL be documented.
- At a minimum, an annual audit of users SHALL be conducted to determine what their effective rights and privileges are (e.g., if a user is a member of several security groups it is possible for that user to have privileges that were not intentional).

6.6 Inactive Sessions

- The inactive time limit SHALL be set to 15 minutes or less.
- All devices not in a controlled access area where only trusted users are able to access the device SHALL have a method in place to lock out or terminate an inactive session when the inactive time limit is reached.
- Once a device is locked or disconnected, reauthentication SHALL be required to reestablish the session or gain access.

6.7 Device Protections

6.7.1 Remote Access Device Security

- Personal devices SHALL **NOT** be connected to a NG9-1-1 system in any way (i.e., charging a phone or plugging in a personal USB).
- Remote access devices that store sensitive information SHALL be encrypted in compliance with Section 4.2.2.6 Safeguarding Sensitive Electronic Information.
- Remote access devices SHALL **NOT** be plugged into unauthorized USB charging ports or devices.
- Remote access devices SHALL use an Entity approved connection using TLS, or optionally VPN when systems require the kind of address access limitations a VPN provides.
- Remote access devices that store sensitive information or have access to a NG9-1-1 system SHALL require domain authentication in accordance with the Authentication/Password policy.
- Remote access devices that store sensitive information or have access to a NG9-1-1 system SHALL be powered off, secured, and concealed from view when left unattended outside of controlled and secured areas.
- Remote access devices that store sensitive information or have access to a NG9-1-1 system SHALL **NOT** be left logged in while not in direct physical control of the authorized user who is logged in.

6.7.2 Environmental Controls

- NG9-1-1 Entities SHALL identify potential environmental risks for each geographic area.
- Each geographic area of a NG9-1-1 Entity SHALL have environmental protection(s) in place for each identified environmental risk. This would include controls like sprinklers, dust filtration, and HVACs.
- A NG9-1-1 Entity SHALL have documented safety plans for each environmental risk. These are plans for events like fire, flood, etc.
- Environmental sensors SHALL be installed and operational that alert personnel when conditions exceed a normal and/or safe operational range. Some examples of these are smoke, temperature, water, and CO2 sensors.
- Fire extinguishers SHALL be easily viewable and accessible from all locations throughout the facility and in accordance with local code.
- An NG9-1-1 Entity SHALL inspect all environmental controls at least annually and in accordance with local code.
- Mission essential NG9-1-1 systems SHALL have surge protection.
- Mission essential NG9-1-1 systems SHALL have a backup battery system.
- NG9-1-1 Entity policy SHALL address the use of food or drink around NG9-1-1 system devices.

6.7.3 Network Infrastructure

- Physical access to rooms containing network infrastructure SHALL be restricted to authorized individuals with a valid business need.
- Rooms containing critical network infrastructure SHALL have HVAC capable of maintaining temperature and humidity within the range specified by the manufacturer(s) for all equipment within the room.
- Physical access to rooms containing power distribution, backup power, and HVAC SHALL be restricted to authorized individuals with a valid business need.
- Active network jacks connecting to a NG9-1-1 system SHALL only be in physically secured areas.
- Unused network jacks connected to a NG9-1-1 system SHALL be disabled or removed.
- Network transport media that could potentially transport and/or access sensitive information SHALL be selected, located, and installed in such a way as to discourage wiretapping, electronic eavesdropping, or tampering. For example, the use of fiber optic cable, coax, and/or enclosed conduit for cable runs could be used.
- Smoking SHALL **NOT** be allowed in rooms containing critical network infrastructure.

6.8 Denial of Service Defense

- NG9-1-1 Entities SHALL have plans to mitigate DoS types of attacks.
- NG9-1-1 Entities SHALL have procedures to handle DoS types of attacks.

6.9 Segmentation

- Production environments SHALL be segmented from non-production environments in such a way as to protect production environments from activity in non-production environments.
- Production environments SHALL **NOT** contain development tools.

6.10 Firewalls

6.10.2 Session Border Controller

- A NENA standard Border Control Function consists of a Session Border Controller and SHOULD include Next-Generation Firewall functionality and SHALL be implemented in NG9-1-1 systems at the ingress and egress of the ESInet and MAY be implemented by any entity.
- A Session Border Controller (SBC) SHALL be implemented to protect all real-time (voice, video, etc.) communications.
- All NG9-1-1 entities SHALL deploy a Next Generation Firewall or SBC at all ingress and egress points not just in the ESInet.
- All entry and exit points for each segment within a NG9-1-1 system SHALL have a Next Generation Firewall or SBC.

- All necessary traffic SHALL be identified and documented for each Next Generation Firewall or SBC.
- All firewalls SHALL explicitly block unnecessary traffic.
- All firewall configurations SHALL be reviewed at least annually.
- Firewall patches and updates SHALL be reviewed at least monthly and applied as soon as possible.
- All NG9-1-1 Entity firewalls SHALL have their times synchronized.
- Firewall logs SHALL be enabled and, at a minimum, record the following:
    - Date/time stamp
    - Unsuccessful firewall logins
    - Successful firewall logins
    - Firewall login disconnects
    - Traffic addressed to the firewall
    - Firewall being stopped, started, or restarted
    - Firewall configuration changes
- Firewall logs SHALL be reviewed daily against an established baseline.
- Firewall logs SHALL be kept for a minimum of 1 year and in accordance with local regulations.
- Firewall logs SHALL be protected from unauthorized deletion or modification.

6.11 External Connections

- External connections SHALL operate off the zero-trust model. For more information on zero-trust see Appendix A – Zero-Trust Architecture.
- External connections SHALL be protected with a firewall in accordance with Section 6.10 Firewalls.
- External connections transporting sensitive information SHALL be protected with encryption in accordance with Section 4.2.2.6 Safeguarding Sensitive Electronic Information.

6.12 Demilitarized Zones (DMZs)

- Externally accessible resources not protected by other means SHALL be placed in a DMZ.

6.13 Defense in Depth

- Critical systems and sensitive information SHALL utilize Defense in Depth.

6.14 Network Availability

- Critical NG9-1-1 systems SHALL have redundancy to ensure the availability of mission critical functions.

6.15 Diversity

- 9-1-1 call traffic SHALL enter a NG9-1-1 system through diverse paths.

- Critical NG9-1-1 systems SHALL have diversity to ensure availability of mission critical functions.

6.16 Traffic Separation

- Management and monitoring of virtual and logical networks SHALL be handled out of band from regular traffic. For example, management and monitoring will use one VLAN while normal traffic flows through another VLAN.
- For virtual separations, normal traffic SHALL **NOT** use the default VLAN.
- Access to configuration settings on devices handling network traffic SHALL utilize an administrator level account. See Section 6.2.1.3 Administrator Accounts.

6.17 Remote Access

- External remote access SHALL be only allowed for those with a valid business need.
- External remote access accounts SHALL be reviewed at least annually.
- All external remote access connections SHALL be through an authorized secured and encrypted connection like a VPN.
- NG9-1-1 Entities SHALL **NOT** use modems for external remote connections.
- All external remote access connections SHALL require multi-factor authentication.
- Domain or system authentication SHALL be required after successfully establishing an authorized external remote connection but before gaining access to any resources. Note: this means there are two authentications. One to establish the connection and one to authenticate to the domain.
- Inactive external remote connections SHALL be terminated after 30 minutes or less of inactivity.
- A NG9-1-1 Entity SHALL log, at a minimum, all external remote access connections successful authentication attempts, failed authentication attempts, source IP, start of session timestamp, and end of session timestamp.

6.18 Intrusion Detection/Prevention

- If a signature-based IDS/IPS is used the signatures SHALL be updated at least weekly. More frequent updates are recommended.
- If an anomaly-based IDS/IPS is used the profiles SHALL be updated at least annually. More frequent updates are recommended as needed.
- Alerts SHALL be reviewed at least weekly.
- Configurations SHALL be reviewed at least annually.

6.19 Endpoint Security

- Endpoints supporting mission critical functions SHALL be hardened.
- Endpoints supporting mission critical functions SHALL be reviewed at least annually to ensure they are still hardened.

6.20 Email

- Mail server(s) SHALL be installed on a dedicated system or systems.

- Mail server(s) SHALL be hardened.
- Email SHALL be scanned for malware.
- Email SHALL have content filtering.
- Call taking workstations SHALL **NOT** be used to send/receive/view email.

6.21 Text, Pictures, and Video 9-1-1 Communication Data

- A NG9-1-1 Entity viewing text messages to 9-1-1 SHALL define how to handle links in 9-1-1 requests.
- Text, pictures, and video SHALL be opened/viewed in a manner that protects critical NG9-1-1 system resources from malicious content.

6.22 Encryption

- NG9-1-1 Entity SHALL use a security algorithm as specified in NENA-STA-010.3 [6].
- NG9-1-1 Entity encryption algorithms and key lengths SHALL be selected such that they are expected to protect that data for the duration the data needs to be protected.

6.23 Cryptography

6.23.7 Cryptographic Keys

- Private keys SHALL be classified as Sensitive (Most Sensitive Information).
- Private keys SHALL be protected from unauthorized disclosure.
- Private keys that are compromised or suspected of being compromised SHALL be revoked and new keys issued if needed.
- All requirements from the NIOC's PCA Certificate Policy are incorporated into this standard by reference and SHALL be adhered to by implementations.
- All requirements from the NIOC's PCA Validation Policy are incorporated into this standard by reference and SHALL be adhered to by implementations.

6.23.8 Self-Signed Certificates

- Self-signed digital certificates (i.e., digital certificates not issued by a Certificate Authority) SHALL **NOT** be used within or between ESInets for NG9-1-1 communications.
- External entities that do not participate in the PCA-traceable PKI that interact with an ESInet SHALL use digital certificates issued by a reputable public Certificate Authority.

6.24 Disposal

- Paper material containing sensitive information SHALL be disposed of in such a way that it is impractical to reconstruct any portion of a document.
- Devices that never held or processed sensitive information SHALL, at a minimum, be reset to factory defaults with all NG9-1-1 data removed.

- Devices that held or processed sensitive information at any point SHALL have their volatile memory cleared and any electronic storage media sanitized.
- Cloud-based storage SHALL have all Sensitive Data being disposed of rendered irretrievable.

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Systems, Security & Resiliency Committee, Security for NG9-1-1 Working Group developed this document.

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Adam Carney	McLean County, IL
Avi Bryan	Seminole County, FL
Bernard Brabant	Consultant-Bernard Brabant
Brady McCamley, Working Group Co-Chair	911 Authority LLC
Brian Beckwith	Intuitus (formerly CBA)
Brian Daly	AT&T
Brian Nelson	911nurd LLC
Cory Golob, ENP	Emergency Services Communication Bureau
Courtney Doberstein ENP	Harrisonburg-Rockingham Emergency Communications Center (HRECC), VA
Dan Mongrain, Eng., Systems Security & Resiliency Committee Co-Chair	Motorola Solutions, Inc.
Hakeem Thomas	Netmaker Communications, LLC
James Lockard, PgMP, PMP, ENP, Working Group Co-Chair	911 Authority LLC
Jerry Eisner	Verizon
Joel McCamley, Sr. ENP	911 Authority, LLC
John Kalinowski, ENP	City of Grand Rapids, MI
Keith Martin	AT&T
Michael Nairn	Broward County, FL
Paresh Patel	Carbyne
Pete Eggimann	Eggimann Technology Services, LLC
Ravi Valavandan, ENP	City of Calgary, AB, CA
Raymond Paddock, Systems Security & Resiliency Committee Co-Chair	Synergem Technologies Inc.
Roger Marshall	Comtech Telecommunications Corporation
Ryan Lanier	**M**obile **C**ounty **C**ommunications **D**istrict, AL
Scott O'Connell, ENP, CISSP	Helena Lewis and Clark 911, MT
Scott Wolfert ENP	Consolidated Communications Inc
Stephen Doyle	Atos Public Safety

Members	Employer
Steve Walsh, CISSP, Working Group Co-Chair	State of Washington 911 Coordination Office
Tom Breen, ENP, Working Group Co-Chair	SecuLore, an Exacom company
William Mertka, ENP	AT&T
William Pellegrini	Intrado - Life & Safety

Special Acknowledgements:

Delaine Arnold, ENP (dec.), and Sandy Dyre, ENP, Committee Resource Managers, have facilitated the production of this document through the prescribed approval process.

The Security for NG9-1-1 Working Group is part of the NENA Development Group that is led by:

- Wendi Rooney-ENP, and Lisa Dodson-ENP, Development Steering Council Co-Chairs, and Jim Shepard-ENP, past Development Steering Council Co-Chair
- Brandon Abley-ENP, Chief Technology Officer
- April Heinze-ENP, VP, Chief of 9 1 1 Operations