NIST CSF 2.0 Crosswalk
NENA-REF-013.1-2025

NENA Reference Publication Number: NENA-REF-013.1-2025
Material type: Checklist

Synopsis of the material Content:
This REF (NENA Reference Publication) is a companion to the NENA-STA-040.2 NENA Security for Next Generation 9-1-1 Standard (NG-SEC) and provides a crosswalk between NIST CSF 2.0 and NENA-STA-040.2.

Expected publication methods: NENA public website
Hyperlink to material: https://www.nena.org/page/standards

Authoring Committee: SS&R-Systems Security & Resiliency Committee
Working Group: SS&R-Security Audit Checklist WG
Issue Submission Form Number: 20240109-2

Date Approved by the DSC: August 5, 2025
Recommended for update: Coincide with changes made to NENA-STA-040.2.

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 nena.org.

Intellectual Property Rights (IPR) Policy

NOTE – The user's attention is called to the possibility that compliance with this document may require use of an invention covered by patent rights. By publication of this document, 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 www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at 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 any standards referenced by this document or to implement or follow any recommended best practices, procedures or architectures contained herein.

Please address the information to:

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

Security Standard Crosswalk Description

This crosswalk provides a best-effort mapping between NENA-STA-040.2-2024 Security for Next Generation 9-1-1 Standard (NG-SEC) and NIST Cybersecurity Framework (CSF) 2.0, released on February 26, 2024. This is laid out in a table format. The first column is a sequential numbering of all requirements used in this document. The second column shows the requirements as stated in NENA-STA-040.2-2024. The Third column lists the section number from NENA-STA-040.2-2024. The fourth column lists the relevant category and subcategories from NIST CSF 2.0 released on February 26, 2024.

The following formatting has been used:

- Blue italic text indicates clarifying text that has been added for clarity of the requirement and may not necessarily be part of the requirement.
- All footnotes that may have been part of a requirement in NENA-STA-040.2-2024 have been removed.
- Bolded text in black in the NIST column indicates areas that were determined to have a strong relationship to the requirement.
- Italicized red text in the NIST column indicates areas that were determined to have a weaker relationship to the requirement.
- If a category (letters with no number) is listed under the NIST column, the entire category applies.
- If a subcategory (letters with a number suffix) is listed under the NIST column, the subcategory applies.

About NIST CSF 2.0

NIST CSF 2.0 builds upon previous versions, introducing refinements and reorganizing categories for better alignment with modern cybersecurity practices. Each category and subcategory are referenced using a unique identifier, which provides a structured approach to managing cybersecurity risks. These reference numbers are used in this crosswalk to illustrate connections between Next Generation 9-1-1 Standard (NG-SEC) and NIST Cybersecurity Framework (CSF) 2.0, released on February 26, 2024.

More information on the NSIT CSF 2.0 can be found at: https://www.nist.gov/cyberframework. Mappings to NIST documents and some other frameworks can be found under Informative References (Mappings).

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
1	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.	3.2	**ID.RA-04** *ID.RA-01* *ID.RA-05* *ID.RA-06*
2	Unresolved non-compliance SHALL require documented risk acceptance as described in Section 4.3 Risk Management.	3.2	**GV.RM-06** **GV.PO-01** *GV.RM-01* *GV.RM-02* *GV.RM-03* *GV.RM-04* *ID.RA-06*
3	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	**GV.RM-06** **GV.PO-01** *GV.RM-01* *ID-RA-01* *ID.RA-05*
4	Every individual within a NG9-1-1 Entity SHALL be informed of 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.	3.4	**GV.RR-02** **GV.PO-01** **PR.AT-02** *GV.RR-01*
5	*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.	3.4	**GV.RR-02** *GV.RR-01* *GV.RR-03* *GV.RR-04*
6	*The following responsibilities SHALL be fulfilled:* 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.	3.4	**GV.RR-02**
7	*The following responsibilities SHALL be fulfilled:* 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.	3.4	**GV.RR-02**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
8	*The following responsibilities SHALL be fulfilled:* 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.	3.4	**GV.RR-02**
9	*The following responsibilities SHALL be fulfilled:* 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.	3.4	**GV.RR-02**
10	*The following responsibilities SHALL be fulfilled:*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.	3.4	**GV.RR-02**
11	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.	4	*GV.SC-02* *GV.SC-05* *GV.SC-07*
12	When outsourcing data or systems that contain data, the contract SHALL clearly define who owns that data.	4	*GV.SC-05* *GV.SC-10* *ID.AM-07* *ID.AM-08*
13	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.	4	*GV.SC-05* *PR.DS-01* *PR.DS-02* *PR.DS-10* *PR.DS-11*
14	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	*GV.OC-03*
15	Senior management SHALL create and model a culture of security as outlined in this document.	4.11	*GV.RR-01* *GV.RR-04*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
16	*The Senior Management SHALL, at a minimum:* Provide documentation defining the security goals and objectives for a NG9-1-1 Entity.	4.11	**GV.PO-01** *GV.RM-01* *GV.OC-01*
17	*The Senior Management SHALL, at a minimum:* Provide the necessary resources to accomplish the security goals and objectives for a NG9-1-1 Entity.	4.11	*GV.RR-03*
18	*The Senior Management SHALL, at a minimum:* Assign the roles and responsibilities for a NG9-1-1 Entity.	4.11	*GV.RR-02*
19	*The Senior Management SHALL, at a minimum:* Retains overall responsibility for a NG9-1-1 Entities security program.	4.11	*GV.RR-01*
20	*The Senior Management SHALL, at a minimum:* Instill and model a NG9-1-1 Entity wide security mind set.	4.11	*GV.RR-01* *GV.RR-04*
21	*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.	4.1.2	**GV.PO-01** *PR.AT-01*
22	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Auditing and Assessment Policy: This policy defines the frequency and scope of security audits and assessments.	4.1.2	**GV.PO-01** *ID.RA-01*
23	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Authentication/Password Policy: This policy defines authentication and password requirements for a NG9-1-1 Entity.	4.1.2	**GV.PO-01** *PR.AA-05* *PR.AA-01* *PR.AA-03*
24	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:*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.	4.1.2	**GV.PO-01** *PR.PS-01* *ID.RA-07*
25	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* 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.	4.1.2	**GV.PO-01** *RS.MA-01* *RS.CO-02*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
26	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* 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.	4.1.2	**GV.PO-01** *PR.DS-01* *PR.DS-02* *ID.AM-07*
27	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Equipment Disposal Policy: This policy defines how equipment will be disposed of.	4.1.2	**GV.PO-01** *PR.PS-03*
28	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Endpoint Protection Policy: This policy defines the security controls and patch management for each type of device.	4.1.2	**GV.PO-01** *PR.PS-01* *PR.PS-02* *PR.PS-05*
29	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* 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.	4.1.2	**GV.PO-01** *GV.RR-04* *PR.AT-01* *PR.AT-02*
30	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Physical Security Policy: This policy defines physical access and theft prevention requirements.	4.1.2	**GV.PO-01** *PR.AA-06*
31	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* 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.	4.1.2	**GV.PO-01** *GV.SC-05* *ID.RA-09* *ID.RA-10*
32	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Remote Access Policies: This policy defines authorized methods for all external remote connections to NG9-1-1.	4.1.2	**GV.PO-01** *PR.AA-05*
33	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Risk Management Policy: This policy defines how risk is assessed resulting from threats to the confidentiality, integrity, and availability of NG9-1-1 assets.	4.1.2	**GV.PO-01** *GV.RM-06* *ID.RA-01*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
34	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Security Awareness Training Policy: This policy defines the frequency and core topics of the Entities security awareness training.	4.1.2	**GV.PO-01** *PR.AT-01* *PR.AT-02*
35	*A NG9-1-1 Entity SHALL, at a minimum, have the following policies:* Security Monitoring Policy: This policy defines logging, endpoint monitoring, and traffic monitoring and how often that information will be reviewed.	4.1.2	**GV.PO-01** *DE.CM-02* *DE.CM-01* *DE.CM-03* *DE.CM-06* *DE.CM-09*
36	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.	4.1.3	*PR.PS-01* *PR.PS-02* *PR.PS-03*
37	SOPs SHALL be developed, maintained, periodically updated, and utilized for all identified tasks.	4.1.3	*PR.PS-01* *ID.IM-03*
38	*The Data Owner SHALL:* Assess the risk associated with the loss of data for which they are the Data Owner.	4.1.4.3	**ID.RA-05** *ID.RA-04*
39	*The Data Owner SHALL:* Judge the value of the data and assign the proper classification level according to the Data Protection Policy.	4.1.4.3	**ID.AM-05**
40	*The Data Owner SHALL:* Periodically review the classification level for all data for which they are the Data Owner to determine if the status should be changed.	4.1.4.3	*ID.RA-07*
41	*The Data Owner SHALL:* Communicate access and control requirements to the Data Custodian and users.	4.1.4.3	**PR.AA-05**
42	*The Data Owner SHALL:* 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).	4.1.4.3	**PR.AA-05**
43	*The Data Owner SHALL:* Ensure that the required security controls are in place to mitigate the risk to data integrity, confidentiality, and availability.	4.1.4.3	**PR.DS-01** **PR.DS-02** **PR.DS-10** *PR.AA-05* *ID.RA-06*
44	*The Data Owner SHALL:* Conduct, at a minimum, an annual audit of all data for which they are the Data Owner.	4.1.4.3	*ID.RA-01* *ID.IM-01*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
45	*The Data Owner SHALL:* Monitor safeguard requirements to ensure that information is being adequately protected.	4.1.4.3	**DE.CM-03** **DE.CM-09** *ID.RA-05*
46	When an employee, vendor, contractor, agent, or service provider retains data, they SHALL become a custodian for that data.	4.1.4.4	**GV.RR-02**
47	*A Data Custodian SHALL:* Ensure data is used as authorized and only for the purpose intended.	4.1.4.4	**PR.AA-05**
48	*A Data Custodian SHALL:* Ensure access by authorized users with a demonstrated business need.	4.1.4.4	**PR.AA-05**
49	*A Data Custodian SHALL:* Maintain the integrity, confidentiality, and availability of the data for which they are the Data Custodian.	4.1.4.4	**PR.DS-01** **PR.DS-02** **PR.DS-10**
50	*A Data Custodian SHALL:* Comply with information classification and protection policies on retention and disposal of records and data.	4.1.4.4	**GV.PO-01** **ID.AM-08**
51	*A Data Custodian SHALL:* Ensure required safeguards are being used for processing equipment, information storage, backup, and recovery.	4.1.4.4	**PR.DS-01** **PR.DS-11** *RC.RP-03*
52	*A Data Custodian SHALL:* Ensure the data is used in an authorized secure processing environment that can adequately protect the integrity, confidentiality, and availability of information.	4.1.4.4	**PR.DS-01** **PR.DS-02** **PR.DS-10**
53	*A Data Custodian SHALL:* Periodically review data access to ensure that it is only authorized users have access and it is being used for the purpose intended.	4.1.4.4	**PR.AA-05** *DE.CM-03*
54	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.	4.2.1	**ID.RA-01** **ID.RA-05**
55	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.	4.2.2.1	*PR.DS*
56	The Data Protection Policy SHALL define which classifications levels the Entity believes are not subject to the Freedom of Information Act (FOIA) or similar laws.	4.2.2.1	**GV.OC-03**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
57	All classified data SHALL be assigned a classification level according to the highest sensitivity of any information in that data set.	4.2.2.1	*ID.AM-05* *PR.DS-01*
58	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.	4.2.2.1	**GV.OC-03** **GV.SC-05** **GV.RR-02** *PR.AA-05*
59	Persons not authorized to view or modify information SHALL be prohibited from viewing or modifying information.	4.2.2.1	**PR.AA-05**
60	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.	4.2.2.1	**GV.SC-05** *PR.AA-05*
61	Access to sensitive information SHALL be reviewed at least annually.	4.2.2.1	**PR.AA-05** *DE.CM-03*
62	Release of Sensitive (Internal Use Only) Data/information SHALL be documented when released.	4.2.2.1.2	**ID.AM-07** *PR.AA-05*
63	Restricted information SHALL be shared only with the explicit permission of the originator.	4.2.2.1.3	**PR.AA-05**
64	*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.	4.2.2.1.3	*PR.AA-05*
65	Release of Sensitive (Restricted) information SHALL be documented when released.	4.2.2.1.3	**ID.AM-07** *PR.AA-05*
66	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.	4.2.2.1.4	**GV.OC-03** **PR.AA-05**
67	Release of Sensitive (Most Sensitive) information SHALL be documented when released subject to an FOIA request.	4.2.2.1.4	**GV.OC-03** **ID.AM-07** *PR.AA-05*
68	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.	4.2.2.3	**PR.AA-05** *DE.CM-03*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
69	External party Sensitive Data SHALL be safeguarded in the same manner as like data for the Entity and classified as such.	4.2.2.4	**PR.DS-01** **PR.DS-02** **PR.DS-10** **PR.AA-05** *GV.SC-05*
70	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. *Defined below refers to data at rest, in transit, and in use.*	4.2.2.5	**GV.PO-01** **PR.DS-01** **PR.DS-02** **PR.DS-10**
71	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.	4.2.2.5.1	**GV.PO-01** *ID.AM-01* *ID.AM-08*
72	Protection of Sensitive Data at rest SHALL be defined in the Data Protection Policy.	4.2.2.5.1	**GV.PO-01** *PR.DS-01*
73	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.	4.2.2.5.1	**PR.DS-01**
74	Disk encryption (full/partial) for Sensitive Data SHALL be defined in the Data Protection Policy. Storing Sensitive Data on CDs/DVDs should be avoided.	4.2.2.5.1	**GV.PO-01** **PR.DS-01**
75	Destruction and/or disposal procedures for Data SHALL be defined in the Disposal Policy.	4.2.2.5.1	**GV.PO-01**
76	Sensitive Data requires encryption as defined in NENA-STA-010.3 and SHALL be defined in the Data Protection Policy.	4.2.2.5.2	**GV.PO-01** *PR.DS-01* *PR.DS-02*
77	Data in use SHALL be safeguarded from unauthorized disclosure.	4.2.2.5.3	**PR.DS-10**
78	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.	4.2.2.5.3	**GV.PO-01** *PR.DS*
79	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).	4.2.2.5.3	**PR.DS-01**
80	All media distributed outside NG9-1-1 Entity SHALL be new or come directly from a recognized pool of "clean" media.	4.2.2.5.3	**PR.DS-01**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
81	*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).	4.2.2.6	**PR.DS-01** *PR.AA-05*
82	*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 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).	4.2.2.6	**PR.DS-01** *PR.AA-05*
83	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.	4.2.2.6	**PR.DS-01** **PR.DS-02**
84	In NG9-1-1 systems, the encryption algorithm SHALL be AES 256.	4.2.2.6	**PR.DS**
85	*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.	4.2.2.6	**PR.DS** *PR.AA-05*
86	*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:* Exceptions to the policy SHALL be documented in writing.	4.2.2.6	**PR.DS** *PR.AA-05*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
87	*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:* 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 nondisclosure agreements, laws, regulations, and policies to ensure that information contained on the devices is safeguarded.	4.2.2.6	**PR.DS** **PR.PS-02** **PR.PS-03** *GV.SC-05* *PR.AA-05*
88	*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).	4.2.2.7	**GV.SC-07** **PR.DS-01** *GV.SC-05*
89	*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).	4.2.2.7	*GV.SC-05* *GV.SC-06* *GV.SC-07* *PR.AA* *PR.DS* *PR.PS-04* *DE.CM*
90	*The cloud vendor provided mechanisms used by NG9-1-1 entities:* SHOULD adhere to broadly accepted security conventions, e.g., NIST-800, CIS Controls, or other locally applicable controls.	4.2.2.7	**GV.PO-01** **GV.SC-05**
91	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.	4.2.3	**PR.DS** *PR.AA-05*
92	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.	4.2.3	**PR.DS** *PR.AA-05*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
93	*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.	4.2.4.1	**PR.DS-01** *PR.AA-05*
94	*Sensitive (Internal Use Only) – Printed Material Inside Controlled Space user(s) SHALL:* Observe sending and receiving fax machines with authorized personnel or use fax machines in offices/areas where access is limited to authorized personnel.	4.2.4.1	**PR.DS-01** **PR.DS-02** *PR.AA-05*
95	*Sensitive (Internal Use Only) – Printed Material Inside Controlled Space user(s) SHALL:* Ensure that Printed Material is shredded when no longer needed.	4.2.4.1	**PR.DS-01** *PR.AA-05*
96	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Ensure Printed Material is secured from unauthorized access.	4.2.4.1	**PR.DS-01** *PR.AA-05*
97	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Ensure Printed Material is kept in the direct supervision of the custodian.	4.2.4.1	**PR.DS-01** *PR.AA-05*
98	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Ensure Printed Material is in direct supervision of the Data Custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).	4.2.4.1	**PR.DS-01** *PR.AA-05*
99	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Observe the printer or copier with an authorized person for the information.	4.2.4.1	**PR.DS-01** *PR.AA-05*
100	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Use a sealed envelope whenever delivery is to a location external to the controlled space or whenever the delivery utilizes non-company personnel or service.	4.2.4.1	**PR.DS-01** *PR.AA-05*
101	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Supervise fax machines that are located outside the controlled space with authorized personnel.	4.2.4.1	**PR.DS-01** *PR.AA-05*
102	*Sensitive (Internal Use Only) – Printed Material Outside Controlled Space user(s) SHALL:* Ensure Printed Material is shredded when no longer needed.	4.2.4.1	**PR.DS-01** *PR.AA-05*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
103	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is kept away from casual observers.	4.2.4.2	**PR.DS-01** *PR.AA-05*
104	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* 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.	4.2.4.2	**PR.DS-01** *PR.AA-05*
105	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* Monitor the printer or copier unless printer/copier is in an office/area where access is limited to authorized personnel.	4.2.4.2	**PR.DS-01** *PR.AA-05*
106	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is hand delivered by originator or Data Custodian.	4.2.4.2	**PR.DS-01** *PR.AA-05*
107	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* Use double envelopes with the inner envelope marked "Private" when using internal mail.	4.2.4.2	**PR.DS-01** *PR.AA-05*
108	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* Supervise sending and receiving fax machines with authorized personnel or use fax machines in offices/areas where access is limited to authorized personnel.	4.2.4.2	**PR.DS-01** *PR.AA-05*
109	*Sensitive (Restricted) – Printed Material* *Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is shredded when no longer needed.	4.2.4.2	**PR.DS-01** *PR.AA-05*
110	*Sensitive (Restricted) – Printed Material* *Outside the Controlled Space user(s) SHALL:* Ensure Printed Material is kept away from casual observers.	4.2.4.2	**PR.DS-01** *PR.AA-05*
111	*Sensitive (Restricted) – Printed Material* *Outside the Controlled Space user(s) SHALL:* 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).	4.2.4.2	**PR.DS-01** *PR.AA-05*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
112	*Sensitive (Restricted) – Printed Material Outside the Controlled Space user(s) SHALL:* Ensure Printed Material is in direct supervision of the Data Custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).	4.2.4.2	**PR.DS-01** *PR.AA-05*
113	*Sensitive (Restricted) – Printed Material Outside the Controlled Space user(s) SHALL:* Monitor the printer or copier with a person authorized for the information.	4.2.4.2	**PR.DS-01** *PR.AA-05*
114	*Sensitive (Restricted) – Printed Material Outside the Controlled Space user(s) SHALL:* Use double envelopes with the inner envelope marked "Private" and send recorded/certified delivery whenever delivery is to a location external to controlled space or whenever the delivery utilizes non-company personnel or service.	4.2.4.2	**PR.DS-01** *PR.AA-05*
115	*Sensitive (Restricted) – Printed Material Outside the Controlled Space user(s) SHALL:* Monitor fax machines that are located outside NG9-1-1 Entity controlled space with authorized personnel.	4.2.4.2	**PR.DS-01** *PR.AA-05*
116	*Sensitive (Restricted) – Printed Material Outside the Controlled Space user(s) SHALL:* Ensure Printed Material is shredded when no longer needed.	4.2.4.2	**PR.DS-01** *PR.AA-05*
117	*Sensitive (Most Sensitive Information) – Printed Material Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is kept away from casual observers.	4.2.4.3	**PR.DS-01** *PR.AA-05*
118	*Sensitive (Most Sensitive Information) – Printed Material Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is kept in the direct supervision of the Data Custodian or physically secured (e.g., desk, filing cabinet, safe).	4.2.4.3	**PR.DS-01** *PR.AA-05*
119	*Sensitive (Most Sensitive Information) – Printed Material Inside the Controlled Space user(s) SHALL:* Monitor the printer or copier, or print/copy in an office/area where access is limited to authorized personnel.	4.2.4.3	**PR.DS-01** *PR.AA-05*
120	*Sensitive (Most Sensitive Information) – Printed Material Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is hand delivered by the originator or Data Custodian.	4.2.4.3	**PR.DS-01** *PR.AA-05*
121	*Sensitive (Most Sensitive Information) – Printed Material Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is not faxed.	4.2.4.3	**PR.DS-01** *PR.AA-05*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
122	*Sensitive (Most Sensitive Information) – Printed Material Inside the Controlled Space user(s) SHALL:* Ensure Printed Material is shredded when no longer needed.	4.2.4.3	**PR.DS-01** *PR.AA-05*
123	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* Ensure Printed Material is never taken outside the controlled space.	4.2.4.3	**PR.DS-01** *PR.AA-05*
124	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Obtain approval from a Senior Manager.	4.2.4.3	**PR.DS-01** *PR.AA-05*
125	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Kept away from casual observers.	4.2.4.3	**PR.DS-01** *PR.AA-05*
126	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Kept in the direct supervision of the custodian or physically secured (e.g., desk, filing cabinet, safe, car trunk/boot, hotel room safe).	4.2.4.3	**PR.DS-01** *PR.AA-05*
127	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Stay in direct supervision of the custodian when traveling on public transport (e.g., Bus, taxi, airplane, checked baggage).	4.2.4.3	**PR.DS-01** *PR.AA-05*
128	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Monitor any print/copy outside the controlled space.	4.2.4.3	**PR.DS-01** *PR.AA-05*
129	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Hand delivered by the data owner or data custodian.	4.2.4.3	**PR.DS-01** *PR.AA-05*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
130	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Not be faxed.	4.2.4.3	**PR.DS-01** *PR.AA-05*
131	*Sensitive (Most Sensitive Information) – Printed Material Outside the Controlled Space user(s) SHALL:* However, if there is an overriding business need to take Printed Material outside the controlled space, then: Ensure Printed Material is shredded when no longer needed.	4.2.4.3	**PR.DS-01** *PR.AA-05*
132	The Data Protection Policy SHALL define what data can be placed in the public domain and what data is exempt from public disclosure.	4.2.5	**GV.PO** **PR.DS**
133	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.	4.2.5	**GV.PO** **PR.DS**
134	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.	4.2.5	**GV.PO**
135	A NG9-1-1 Entity SHALL have a documented Risk Management process that, at a minimum, evaluates vulnerabilities, threats, and risks.	4.3	**GV.RM** **ID.RA**
136	A NG9-1-1 Entity SHALL have a documented risk acceptance form.	4.3	**GV.RM-06**
137	There SHALL be a risk acceptance form covering every identified risk the entity has direct control over.	4.3	**GV.RM-06**
138	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.	4.3	**GV.RM-01** *GV.RR-01* *GV.RR-02*
139	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	**GV.OV** *ID.RA-05*
140	The PSAP and authority having jurisdiction SHALL ensure that Service Level Agreement(s) (SLA) addresses all threat vectors.	4.3.1	**GV.SC-05** *PR.IR*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
141	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.	4.4	**ID.RA-07** **PR.PS-01** *PR.PS-02* *PR.PS-03*
142	All changes to equipment and/or configuration of a NG9-1-1 system SHALL include a documented security review.	4.4	**ID.RA-07** **PR.PS-01** *PR.PS-02* *PR.PS-03*
143	All changes SHALL be documented. This may consist of new documentation for new equipment or updates to existing documents for configuration changes.	4.4	**ID.RA-07** **PR.PS-01** *ID.AM*
144	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.	5.1.1	**PR.AT**
145	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.	5.1.1	**PR.AT**
146	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.	5.1.2	**PR.AT-02** *GV.SC-05*
147	A security assessment SHALL be conducted, at a minimum, annually. This may be an internal or external assessment.	5.2	**ID.RA-01**
148	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.	5.2	**ID.RA-01**
149	An external assessment, to include gap analysis, SHALL be documented and provided to a NG9-1-1 Security Manager or their designated representative.	5.2	**ID.RA-01** *GV.RM-06*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
150	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.	5.2	**ID.RA-06** **ID.RA-07**
151	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.	5.2	**GV.PO-01**
152	*An inventory SHALL, at a minimum, document and track the following:* *Devices* o Device name o Identification (make, model, and serial number) o End of life date o Firmware version(s) (a device may have multiple components with firmware) o Primary owner/responsible party o Primary location o Highest classification level of data used on/by device o Contract/warranty	5.4	**ID.AM-01** *ID.AM-08*
153	*An inventory SHALL, at a minimum, document and track the following:* *Software and applications* o Software/application name o Software/application version o Number of licenses o End of life date o Device(s) installed on o Highest classification level of data used on/by software/application o Contract/warranty	5.4	**ID.AM-02** *ID.AM-08*
154	*An inventory SHALL, at a minimum, document and track the following:Data (by group)* o Classification level o Storage location o Data Owner o Data Custodian	5.4	**ID.AM-07** *ID.AM-08*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
155	*An inventory SHALL, at a minimum, document and track the following:* *Cloud/third-party services* o Provider o Contact info o Service provided (i.e., data storage, CPE, e-mail, connectivity) o Contract end date o Entity administrator/point of contact o Highest classification level of data on or used by service o Contract/warranty	5.4	**ID.AM-04** *ID.AM-08*
156	*An inventory SHALL, at a minimum, document and track the following:* *Software libraries* o Path o Manufacturer o Version number	5.4	**ID.AM-02** *ID.AM-08*
157	A NG9-1-1 Entity SHALL validate all necessary patches are installed at least monthly.	5.5	**PR.PS-02**
158	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.	5.5	**PR.PS-02**
159	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.	5.5	**RS.MI-02** *ID.RA-06* *ID.RA-07* *ID.RA-08* *DE.AE-02*
160	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.	5.5	**GV.PO-01** *PR.PS-02*
161	Time synchronization SHALL be in accordance with the Time Server specifications in NENA-STA-010.3.	5.6.1	*PR.PS-01* *PR.PS-04*
162	*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.	5.6.2	*PR.PS-01*
163	*Each NG9-1-1 Entity SHALL:* 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.	5.6.2	**PR.PS-04** **DE.CM-09** *DE.CM-01*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
164	*Each NG9-1-1 Entity SHALL:* 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.	5.6.2	**PR.PS-04** **DE.CM-09** *DE.CM-01*
165	*Each NG9-1-1 Entity SHALL:* Protect logs from unauthorized deletion or modification.	5.6.2	**PR.DS**
166	*Each NG9-1-1 Entity SHALL:* Retain logs in accordance with local retention requirements.	5.6.2	**GV.PO-01** *GV.OC-03*
167	There SHALL be a defined process or procedure identifying when and how often the periodic review of security monitoring systems will be done.	5.6.4	**GV.PO-01**
168	A NG9-1-1 Entity SHALL have a Cybersecurity Incident Response plan.	5.6.5	**GV.PO-01** *RS.MA-01*
169	*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.* o Business Continuity plan o Disaster Recovery plan o Cybersecurity Incident Response plan	5.7	**GV.PO-01**
170	*These plans SHALL be maintained offline and be accessible to recovery teams.* o Business Continuity plan o Disaster Recovery plan o Cybersecurity Incident Response plan	5.7	**GV.PO-01**
171	*These plans SHALL be reviewed at least annually and updated as needed.* o Business Continuity plan o Disaster Recovery plan o Cybersecurity Incident Response plan	5.7	**GV.PO-02**
172	A NG9-1-1 Entity SHALL have documented procedures outlining what forensic evidence should be captured and preserved.	5.7.1	**GV.PO-01**
173	A NG9-1-1 Entity SHALL have documented procedures outlining how forensic evidence should be captured.	5.7.1	**GV.PO-01**
174	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.	5.7.1	**GV.PO-01**
175	A NG9-1-1 Entity SHALL have a documented backup plan.	5.7.2.2	**GV.PO-01**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
176	A NG9-1-1 Entity SHALL have documented recovery procedures.	5.7.2.2	**GV.PO-01**
177	A NG9-1-1 Entity SHALL test their backup plan annually at a minimum.	5.7.2.2	**PR.DS-11**
178	All NG9-1-1 Entity information resources SHALL be kept physically secured and protected from theft, misappropriation, misuse, unauthorized access, and damage.	6.1	**PR.AA-06**
179	A controlled area entry and exit log SHALL be maintained for every controlled area.	6.1	**PR.AA-06**
180	Physical access control devices/keys issued to an individual SHALL never be loaned or shared with another individual.	6.1	**GV.PO-01**
181	A person possessing an access control device/key SHALL never use that device/key to allow access to an unauthorized individual.	6.1	**GV.PO-01**
182	NG9-1-1 facilities SHALL have adequate perimeter access control. These may include fencing, video cameras, lighting, guarded access points, etc.	6.1.1	**PR.AA-06**
183	The perimeter of a physically secure location SHALL be prominently posted and separated from non-secure locations by physical controls.	6.1.1	**PR.AA-06**
184	All entry points to secured locations SHALL be prominently marked.	6.1.1	**PR.AA-06**
185	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.	6.1.2	**PR.AA-06**
186	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.	6.1.2	**GV.PO-01** *PR.AA-01*
187	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.	6.1.2	**GV.RR-04**
188	Non-NG9-1-1 Entity employee documentation SHALL be retained for a duration defined by the local retention policy.	6.1.2	**GV.PO-01**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
189	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.	6.1.3	**PR.AA-06**
190	Everyone entering a controlled access facility SHALL follow the physical access control procedures in place for that facility.	6.1.3	**GV.PO-01** *PR.AA-06*
191	A controlled area entry and exit log SHALL be maintained of everyone entering and exiting a controlled area.	6.1.3	**GV.PO-01** *PR.AA-06*
192	Controlled area entry and exit log files SHALL be retained for a duration defined by the local retention policy.	6.1.3	**GV.PO-01**
193	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.	6.1.3	**GV.PO-01** *PR.AA-06*
194	Doors to controlled access areas SHALL NOT be propped open.	6.1.3	**GV.PO-01**
195	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.	6.1.3	**GV.PO-01** *PR.AA-06*
196	Physical access control devices/keys issued to an individual SHALL never be loaned or shared with another individual.	6.1.3	*PR.AA-05* *PR.AA-06*
197	A person possessing an access control device/key SHALL never use that device/key to allow access to an unauthorized individual.	6.1.3	*PR.AA-05* *PR.AA-06*
198	A NG9-1-1 entity SHALL control physical access to information system distribution and transmission lines within a physically secure location.	6.1.4	**PR.AA-06**
199	A NG9-1-1 Entity SHALL control physical access to information system devices.	6.1.5	**PR.AA-06**
200	A NG9-1-1 Entity SHALL position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing.	6.1.5	**PR.AA-06**
201	A NG9-1-1 Entity SHALL monitor physical access to the information system to detect and respond to physical security incidents.	6.1.6	**PR.AA-06**
202	NG9-1-1 Entity employees, authorized non NG9-1-1 employees, and visitors SHALL be issued an identification badge.	6.1.7	**PR.AA**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
203	Employee and authorized non-employee's identification badges SHALL display a picture of the individual the card was issued to.	6.1.7	**PR.AA**
204	The issuance of temporary badges for authorized employees who do not have their official badge SHALL follow local policy and procedures.	6.1.7	**PR.AA**
205	The issuance of a visitor badge SHALL follow local policy and procedures.	6.1.7	**PR.AA**
206	Individuals with visitor badges SHALL be escorted while within non-public areas.	6.1.7	**PR.AA**
207	Visitor and temporary badges SHALL be easily and clearly identifiable.	6.1.7	**PR.AA**
208	Identification badges SHALL be prominently displayed while within NG9-1-1 Entity premises.	6.1.7	**PR.AA**
209	If entry points are staffed, identification badges SHALL be presented to the individual at the entry point prior to being allowed in.	6.1.7	**PR.AA**
210	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.	6.1.7	**PR.AA**
211	Visitor and temporary badges SHALL be turned in when leaving a NG9-1-1 facility.	6.1.7	**PR.AA**
212	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.	6.1.7	**PR.AA**
213	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).	6.1.8	**PR.AA-03** **PR.AA-06** *PR.AA-01*
214	The NG9-1-1 Entity SHALL always escort visitors and monitor visitor activity.	6.1.8	**PR.AA-06**
215	A NG9-1-1 Entity SHALL authorize and control information system-related items entering and exiting the physically secure location.	6.1.9	**PR.AA-06**
216	Each user SHALL have a unique account.	6.2	**PR.AA-01** *PR.AA-05*
217	All guest and/or anonymous accounts SHALL be disabled.	6.2	**PR.AA-01** **PR.AA-05**
218	Role-based access controls SHALL be used.	6.2	**PR.AA-05**
219	Role-based access controls SHALL be reviewed at least annually.	6.2	**PR.AA-05**
220	Creation or modification of accounts SHALL be approved by an authorized representative of a NG9-1-1 Entity.	6.2.1	**PR.AA-01** **PR.AA-05**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
221	Requests for the creation of and/or modification to accounts SHALL be made through an established process that is documented and audited.	6.2.1	**PR.AA-01** **PR.AA-05**
222	Individuals administrating accounts SHALL ensure that only approved creation or changes to accounts are made.	6.2.1	**PR.AA-01** **PR.AA-05**
223	The identity of users requesting password resets SHALL be validated before providing any password reset services.	6.2.1	**PR.AA-04**
224	*The following actions are taken when a user's job assignment changes:* The user's manager SHALL, within one working day, notify account manager(s)/administrator(s) of the change.	6.2.1.1	**PR.AA-01** **PR.AA-05**
225	*The following actions are taken when a user's job assignment changes:* 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.	6.2.1.1	**PR.AA-01** **PR.AA-05**
226	*The following actions are taken when a user's job assignment changes:* 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.	6.2.1.1	**PR.AA-01** **PR.AA-05**
227	*The following actions are taken when a user's job assignment changes:* 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.	6.2.1.1	**PR.AA-01** **PR.AA-05**
228	*The following actions are taken when a user's job assignment changes:* 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.	6.2.1.1	**PR.AA-01** **PR.AA-05**
229	*The following actions are taken when a user's job assignment changes:* All accounts SHALL be reviewed at least annually for authorized privileges and access.	6.2.1.1	**PR.AA-01** **PR.AA-05**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
230	*The following actions are taken when a user's job assignment changes:* Any changes SHALL be reported to the account manager(s)/administrator(s) by an authorized representative.	6.2.1.1	**PR.AA-01** **PR.AA-05**
231	*The following actions are taken when a user's job assignment changes:* Any identified changes SHALL be completed by the account manager(s)/administrator(s) within one working day.	6.2.1.1	**PR.AA-01** **PR.AA-05**
232	All accounts SHALL have a valid business need.	6.2.1.2	**PR.AA-02** *PR.AA-05*
233	All accounts SHALL be approved by an authorized representative.	6.2.1.2	**PR.AA-01** **PR.AA-05**
234	All accounts SHALL be checked at least monthly for inactivity.	6.2.1.2	**PR.AA-01** **PR.AA-05**
235	All accounts SHALL be reviewed at least annually.	6.2.1.2	**PR.AA-01** **PR.AA-05**
236	Unused accounts SHALL be disabled and deleted in accordance with a NG9-1-1 Entity's procedures.	6.2.1.2	**PR.AA-01** **PR.AA-05**
237	All accounts SHALL have a unique password that conforms with the Authentication/Password policy.	6.2.1.2	**PR.AA-01** **PR.AA-05**
238	All account passwords SHALL be changed in accordance with the Authentication/Password policy.	6.2.1.2	**PR.AA-01** **PR.AA-05**
239	Accounts with temporary passwords SHALL require a password change upon first login with the account.	6.2.1.2	**PR.AA-01** **PR.AA-05**
240	Administrator permissions SHALL only be granted to authorized individuals with a valid business need.	6.2.1.3	**PR.AA-02** *PR.AA-05*
241	Administrator accounts SHALL only be used to conduct official NG9-1-1 activities.	6.2.1.3	**PR.AA-05**
242	Administrator accounts SHALL NOT be used for day-to-day user level activities.	6.2.1.3	**PR.AA-05**
243	Administrator accounts SHALL only be used to perform an authorized activity requiring elevated permission.	6.2.1.3	**PR.AA-05**
244	Local administrator accounts SHALL NOT be used when individual domain administrator accounts are an option.	6.2.1.3	**PR.AA-05**
245	Non-unique local and domain administrator accounts (i.e., default admin accounts) SHALL only be used during initial installation or under disaster recovery scenarios.	6.2.1.3	**PR.AA-05**
246	Accounts that have been inactive for 30 days or more SHALL be reviewed.	6.2.1.4	**PR.AA-01** **PR.AA-05**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
247	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.	6.2.1.4	**PR.AA-01** **PR.AA-05**
248	A service account SHALL NOT be used as a user account.	6.2.1.5	**PR.AA-05**
249	A user or administrator account SHALL NOT be used as a service account.	6.2.1.5	**PR.AA-05**
250	Each service account SHALL be documented sufficiently to identify what it is used for and where it is used.	6.2.1.5	**PR.AA-05**
251	A service account SHALL only have the required permissions and access required to perform the action for which it was made (least privilege).	6.2.1.5	**PR.AA-05**
252	Each service account SHALL be dedicated to a single service.	6.2.1.5	**PR.AA-05**
253	Service accounts SHALL be prevented from interactive login unless there is a specific business need.	6.2.1.5	**PR.AA-05**
254	Guest and Anonymous accounts on NG9-1-1 networks and systems SHALL be disabled.	6.2.1.6	**PR.AA-01** **PR.AA-05**
255	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.	6.2.2	**PR.AA-05**
256	Access to all systems from external or remote connections SHALL utilize multi-factor login authentication.	6.2.3	**PR.AA-03** **PR.AA-04**
257	All users of a NG9-1-1 system SHALL be required to authenticate before being allowed access.	6.2.3	**PR.AA-03** **PR.AA-04**
258	User passwords SHALL NOT be visibly displayed when entered.	6.2.3	**PR.AA-05**
259	Failed authentications SHALL NOT identify the reason for the failure.	6.2.3	**PR.AA-05**
260	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.	6.2.3	**PR.AA-05**
261	Passwords SHALL NOT be hard coded into login sequences or scripts.	6.2.3	**PR.AA-05**
262	NG9-1-1 Entity SHALL develop legally acceptable banner messages.	6.2.4	*GV.OC-03*
263	NG9-1-1 Entity devices SHALL display a banner message during the log in sequence.	6.2.4	*GV.OC-03*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
264	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.	6.2.4	*GV.OC-03*
265	Users SHALL NOT use their Passwords/Passphrases for any other account they may have.	6.2.5	**PR.AA-05**
266	Passwords/Passphrases SHALL consist of 16 or more characters.	6.2.5	**GV.PO-02**
267	Passphrases SHALL consist of a minimum of three different words or word segments. These should be words that do not typically go together.	6.2.5	*GV.PO-02*
268	A Passwords/Passphrases SHALL consist of upper-case letters, lower-case letters, numbers, and symbols.	6.2.5	*GV.PO-02*
269	Passwords/Passphrases SHALL NOT consist of sequential characters or words that repeat three or more times.	6.2.5	*GV.PO-02*
270	Passwords/Passphrases SHALL be changed if they are expected to have been compromised.	6.2.5	*GV.PO-02*
271	Only password managers approved by the Security Manager SHALL be used.	6.2.6	*GV.PO-02*
272	Multi-factor authentication SHALL be required to gain access to any password manager.	6.2.6	*GV.PO-02*
273	A user's password manager SHALL NOT be shared with another user.	6.2.6	*GV.PO-02* *PR.AA-05*
274	Users SHALL report the loss or suspected compromise of a password manager within one working day of discovery.	6.2.6	*GV.PO-02* *PR.AA-05*
275	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.	6.2.6	*GV.PO-02* *PR.AA-05*
276	A NG9-1-1 Entity SHALL maintain current documentation on all connections to their NG9 1-1 system.	6.3	**ID.AM-03**
277	All connections transporting sensitive information SHALL be secured (e.g., CJIS, HR, NGCS, CHFE).	6.3	**PR.AA-06** **PR.IR-01**
278	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 in STA-040.2.	6.3.1	**ID.AM-03** **PR.IR-01** **DE.CM-01** **DE.CM-09** *GV.PO-02* *PR.PS-04*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
279	*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.	6.3.2	**PR.IR-01** *PR.AA-05*
280	*If a NG9-1-1 Entity decides to implement Wi-Fi then they SHALL, at a minimum, take the following actions:* 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).	6.3.2	**PR.IR-01**
281	*If a NG9-1-1 Entity decides to implement Wi-Fi then they SHALL, at a minimum, take the following actions:* Disable device management over Wi-Fi.	6.3.2	**PR.IR-01**
282	*If a NG9-1-1 Entity decides to implement Wi-Fi then they SHALL, at a minimum, take the following actions:* Use WPA2-PSK-AES (current standard as of this writing) or stronger standard with a strong password in accordance with the Authentication/Password Policy.	6.3.2	**PR.IR-01** *PR.AA-05*
283	*If a NG9-1-1 Entity decides to implement Wi-Fi then they SHALL, at a minimum, take the following actions:*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.	6.3.2	**PR.IR-01** *PR.AA-05*
284	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.	6.3.3	**PR.DS-02** **PR.IR-01**
285	If a NG9-1-1 Entity incorporates broadband cellular they SHALL ensure the connection has appropriate security.	6.3.4	**PR.IR-01**
286	P2P SHALL only be allowed for those programs or applications that cannot achieve their legitimate business purpose or mission in any other way.	6.3.5	**PR.IR-01**
287	If P2P is allowed, a NG9-1-1 Entity SHALL ensure there is a control in place to validate and verify the information.	6.3.5	*GV.SC-07* *PR.IR-01*
288	If P2P is allowed, a NG9-1-1 Entity SHALL limit the P2P sharing to a NG9-1-1 domain.	6.3.5	**PR.IR-01**
289	NG9-1-1 Entities SHALL enable DNSSEC on all network DNS servers.	6.4	**PR.IR-01**
290	NG9-1-1 Entity clients SHALL request DNSSEC validation.	6.4	**PR.IR-01**
291	NG9-1-1 Entity zone transfers SHALL be restricted to only authorized servers. This SHOULD be accomplished through access control lists.	6.4	**PR.IR-01**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
292	NG9-1-1 Entity DNS servers SHALL have DNS logging enabled.	6.4	**PR.IR-01** **DE.CM-01**
293	NG9-1-1 Entity DNS servers SHALL have the DNS cache locked and set to 100% of time to live.	6.4	**PR.IR-01**
294	NG9-1-1 Entity DNS name servers SHALL have response time limits set.	6.4	**PR.IR-01**
295	Primary DNS servers SHALL NOT be publicly accessible.	6.4	**PR.IR-01**
296	Only authorized administrators SHALL have access to primary DNS servers. This SHOULD be accomplished through access control lists.	6.4	**PR.AA** **PR.IR-01**
297	Publicly accessible DNS servers SHALL be authoritative-only.	6.4	**PR.IR-01**
298	All accounts with privileged access to DNS SHALL follow administrative account requirements. See Section 6.2.1.3 Administrator Accounts.	6.4	**PR.AA**
299	All NG9-1-1 Entity DNS servers SHALL follow patching and updating requirements. See Section 5.5 Patching and Updating.	6.4	**PR.PS-02** *ID.RA-06* *ID.RA-07* *ID.RA-08*
300	Access to data SHALL be limited only to those whose roles require access.	6.5	**PR.AA-05**
301	Privileged access to Sensitive Data SHALL only be given to those with a valid need to know.	6.5	**PR.AA-05**
302	Users SHALL only be given the minimum permissions necessary to perform their job, also known as the principle of least privilege.	6.5	**PR.AA-05**
303	Role based access SHALL be used to assign rights and privileges and SHALL be documented.	6.5	**PR.AA-05**
304	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).	6.5	**PR.AA-05**
305	The inactive time limit SHALL be set to 15 minutes or less.	6.6	**PR.AA-06** *PR.AA-05*
306	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.	6.6	*PR.AA-05* *PR.AA-06*
307	Once a device is locked or disconnected, reauthentication SHALL be required to reestablish the session or gain access.	6.6	**PR.AA-03**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
308	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).	6.7.1	**PR.IR-01**
309	Remote access devices that store sensitive information SHALL be encrypted in compliance with Section 4.2.2.6 Safeguarding Sensitive Electronic Information.	6.7.1	**PR.DS-01** **PR.DS-02** **PR.DS-10**
310	Remote access devices SHALL NOT be plugged into unauthorized USB charging ports or devices.	6.7.1	**PR.IR-01**
311	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.	6.7.1	**PR.IR-01**
312	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.	6.7.1	**PR.AA-03**
313	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.	6.7.1	**PR.AA-06**
314	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.	6.7.1	**PR.AA-06**
315	NG9-1-1 Entities SHALL identify potential environmental risks for each geographic area.	6.7.2	**PR.IR-02**
316	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.	6.7.2	**PR.IR-02**
317	A NG9-1-1 Entity SHALL have documented safety plans for each environmental risk. These are plans for events like fire, flood, etc.	6.7.2	**PR.IR-02**
318	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.	6.7.2	**PR.IR-02**
319	Fire extinguishers SHALL be easily viewable and accessible from all locations throughout the facility and in accordance with local code.	6.7.2	**PR.IR-02**
320	An NG9-1-1 Entity SHALL inspect all environmental controls at least annually and in accordance with local code.	6.7.2	**PR.IR-02**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
321	Mission essential NG9-1-1 systems SHALL have surge protection.	6.7.2	**PR.IR-03**
322	Mission essential NG9-1-1 systems SHALL have a backup battery system.	6.7.2	**PR.IR-03**
323	NG9-1-1 Entity policy SHALL address the use of food or drink around NG9-1-1 system devices.	6.7.2	**GV.PO-01** *PR.IR-02*
324	Physical access to rooms containing network infrastructure SHALL be restricted to authorized individuals with a valid business need.	6.7.3	**PR.AA-06**
325	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.	6.7.3	**PR.IR-02**
326	Physical access to rooms containing power distribution, backup power, and HVAC SHALL be restricted to authorized individuals with a valid business need.	6.7.3	**PR.AA-06**
327	Active network jacks connecting to a NG9-1-1 system SHALL only be in physically secured areas.	6.7.3	**PR.IR-01**
328	Unused network jacks connected to a NG9-1-1 system SHALL be disabled or removed.	6.7.3	**PR.IR-01**
329	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.	6.7.3	**PR.IR-01**
330	Smoking SHALL NOT be allowed in rooms containing critical network infrastructure.	6.7.3	**PR.IR-02**
331	NG9-1-1 Entities SHALL have plans to mitigate DoS types of attacks.	6.8	**PR.IR-03**
332	NG9-1-1 Entities SHALL have procedures to handle DoS types of attacks.	6.8	**RS.MI-01**
333	Production environments SHALL be segmented from non-production environments in such a way as to protect production environments from activity in non-production environments.	6.9	**PR.IR-01**
334	Production environments SHALL NOT contain development tools.	6.9	**PR.IR-01**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
335	A NENA STA-040.2 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.	6.10.2	**PR.IR-01**
336	A Session Border Controller (SBC) SHALL be implemented to protect all real-time (voice, video, etc.) communications.	6.10.2	**PR.IR-01**
337	All NG9-1-1 entities SHALL deploy a Next Generation Firewall or SBC at all ingress and egress points not just in the ESInet.	6.10.2	**PR.IR-01**
338	All entry and exit points for each segment within a NG9-1-1 system SHALL have a Next Generation Firewall or SBC.	6.10.2	**PR.IR-01**
339	All necessary traffic SHALL be identified and documented for each Next Generation Firewall or SBC.	6.10.2	**ID.AM-03** *PR.PS-01*
340	All firewalls SHALL explicitly block unnecessary traffic.	6.10.2	**PR.PS-01** **PR.IR-01**
341	All firewall configurations SHALL be reviewed at least annually.	6.10.2	**GV.PO-01** **PR.PS-01**
342	Firewall patches and updates SHALL be reviewed at least monthly and applied as soon as possible.	6.10.2	**PR.PS-02** **PR.PS-03**
343	All NG9-1-1 Entity firewalls SHALL have their times synchronized.	6.10.2	**PR.PS-01**
344	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Date/time stamp	6.10.2	**PR.PS-04** *DE.CM-01*
345	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Unsuccessful firewall logins	6.10.2	**PR.PS-04** *DE.CM-01*
346	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Successful firewall logins	6.10.2	**PR.PS-04** *DE.CM-01*
347	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Firewall login disconnects	6.10.2	**PR.PS-04** *DE.CM-01*
348	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Traffic addressed to the firewall	6.10.2	**PR.PS-04** *DE.CM-01*

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
349	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Firewall being stopped, started, or restarted	6.10.2	**PR.PS-04** *DE.CM-01*
350	*Firewall logs SHALL be enabled and, at a minimum, record the following:* Firewall configuration changes	6.10.2	**PR.PS-04** *DE.CM-01*
351	Firewall logs SHALL be reviewed daily against an established baseline.	6.10.2	**DE.CM-01**
352	Firewall logs SHALL be kept for a minimum of 1 year and in accordance with local regulations.	6.10.2	**GV.PO-01**
353	Firewall logs SHALL be protected from unauthorized deletion or modification.	6.10.2	**PR.DS**
354	External connections SHALL operate off the zero-trust model. For more information on zero-trust see Appendix A – Zero-Trust Architecture in STA-040.2.	6.11	**PR.AA-04** **PR.IR-01**
355	External connections SHALL be protected with a firewall in accordance with Section 6.10 Firewalls.	6.11	**PR.IR-01**
356	External connections transporting sensitive information SHALL be protected with encryption in accordance with Section 4.2.2.6 Safeguarding Sensitive Electronic Information.	6.11	**PR.DS-02**
357	Externally accessible resources not protected by other means SHALL be placed in a DMZ.	6.12	**PR.IR-01**
358	Critical systems and sensitive information SHALL utilize Defense in Depth.	6.13	**PR.IR-01** *ID.AM-05*
359	Critical NG9-1-1 systems SHALL have redundancy to ensure the availability of mission critical functions.	6.14	**PR.IR-03** *ID.AM-05*
360	9-1-1 call traffic SHALL enter a NG9-1-1 system through diverse paths.	6.15	**PR.IR-03**
361	Critical NG9-1-1 systems SHALL have diversity to ensure availability of mission critical functions.	6.15	**PR.IR-03** *ID.AM-05*
362	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.	6.16	**PR.IR-01**
363	For virtual separations, normal traffic SHALL NOT use the default VLAN.	6.16	**PR.IR-01**
364	Access to configuration settings on devices handling network traffic SHALL utilize an administrator level account. See Section 6.2.1.3 Administrator Accounts.	6.16	**PR.AA-05**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
365	External remote access SHALL be only allowed for those with a valid business need.	6.17	**GV.PO-01** **PR.IR-01**
366	External remote access accounts SHALL be reviewed at least annually.	6.17	**PR.AA-05**
367	All external remote access connections SHALL be through an authorized secured and encrypted connection like a VPN.	6.17	**PR.DS-02** **PR.IR-01**
368	NG9-1-1 Entities SHALL NOT use modems for external remote connections.	6.17	**PR.IR-01**
369	All external remote access connections SHALL require multi-factor authentication.	6.17	**PR.AA-03**
370	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.	6.17	**PR.AA-03** **PR.AA-04**
371	Inactive external remote connections SHALL be terminated after 30 minutes or less of inactivity.	6.17	**GV.PO-01**
372	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.	6.17	**PR.PS-04** **DE.CM**
373	If a signature-based IDS/IPS is used the signatures SHALL be updated at least weekly. More frequent updates are recommended.	6.18	**GV.PO-01**
374	If an anomaly-based IDS/IPS is used the profiles SHALL be updated at least annually. More frequent updates are recommended as needed.	6.18	**GV.PO-01**
375	Alerts SHALL be reviewed at least weekly.	6.18	**GV.PO-01**
376	Configurations SHALL be reviewed at least annually.	6.18	**GV.PO-01**
377	Endpoints supporting mission critical functions SHALL be hardened.	6.19	**PR.PS-01** *ID.AM-05*
378	Endpoints supporting mission critical functions SHALL be reviewed at least annually to ensure they are still hardened.	6.19	**GV.PO-01**
379	Mail server(s) SHALL be installed on a dedicated system or systems.	6.20	*PR.PS*
380	Mail server(s) SHALL be hardened.	6.20	**PR.PS-01**
381	Email SHALL be scanned for malware.	6.20	**DE.CM-09**
382	Email SHALL have content filtering.	6.20	**DE.CM-09**
383	Call taking workstations SHALL NOT be used to send/receive/view email.	6.20	**GV.PO-01**

#	Requirement	NENA- STA-040.2-2024	NIST CSF 2.0
384	A NG9-1-1 Entity viewing text messages to 9-1-1 SHALL define how to handle links in 9-1-1 requests.	6.21	**GV.PO-01**
385	Text, pictures, and video SHALL be opened/viewed in a manner that protects critical NG9-1-1 system resources from malicious content.	6.21	**PR.IR-01**
386	NG9-1-1 Entity SHALL use a security algorithm as specified in NENA-STA-010.3.	6.22	**PR.DS** *PR.PS-02*
387	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.	6.22	**GV-PO-01** **PR.DS** *ID.RA-04*
388	Private keys SHALL be classified as Sensitive (Most Sensitive Information).	6.23.7	**GV-PO-01**
389	Private keys SHALL be protected from unauthorized disclosure.	6.23.7	**PR.DS**
390	Private keys that are compromised or suspected of being compromised SHALL be revoked and new keys issued if needed.	6.23.7	**GV-PO-01**
391	All requirements from the NIOC's PCA Certificate Policy are incorporated into this standard by reference and SHALL be adhered to by implementations.	6.23.7	**GV-PO-01**
392	All requirements from the NIOC's PCA Validation Policy are incorporated into this standard by reference and SHALL be adhered to by implementations.	6.23.7	**GV-PO-01**
393	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.	6.23.8	**GV-PO-01**
394	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.	6.23.8	**GV-PO-01**
395	Paper material containing sensitive information SHALL be disposed of in such a way that it is impractical to reconstruct any portion of a document.	6.24	**PR.DS-01**
396	Devices that never held or processed sensitive information SHALL, at a minimum, be reset to factory defaults with all NG9-1-1 data removed.	6.24	**GV-PO-01**
397	Devices that held or processed sensitive information at any point SHALL have their volatile memory cleared and any electronic storage media sanitized.	6.24	**GV-PO-01** **PR.DS-01**
398	Cloud-based storage SHALL have all Sensitive Data being disposed of rendered irretrievable.	6.24	**GV-PO-01** **PR.DS-01**

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) Systems, Security & Resiliency Committee, Security Audit Checklist Working Group developed this document.

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

Development Steering Council Approval Date: August 5, 2025

Members	Employer
Dan Mongrain, SS&R-Systems Security & Resiliency Committee Co-Chair	Motorola Solutions Inc
Raymond Paddock, SS&R-Systems Security & Resiliency Committee Co-Chair	Synergem Technologies Inc.
Steve Walsh, CISSP Working Group Co-Chair	State of Washington 911 Coordination Office
Tom Breen, ENP Working Group Co-Chair	SecuLore, an Exacom Company
Bill Mertka, ENP	AT&T
Brian Beckwith	Intuitus
Carrie Mills	Comtech
Danny Willars	Tarrant County 9-1-1 District, TX
Greg Platek	Greater Harris County Emergency Network, TX
Jason Jeffares, ENP	911 Authority, LLC
Jason Franks, CISM, CCISO, CRISC	Mission Critical Partners, LLC
Jim Lockard, ENP	911 Authority, LLC
John Kalinowski, ENP, CMCP	City of Grand Rapids, MI
Matt Pence	Oakland County, MI
Pete Eggimann, ENP	Eggimann Technology Services, LLC
Rebecca Anderson	Morris County, KS
Scott O'Connell, ENP, CISSP	Helena Lewis and Clark 911, MT
Stephen Kennedy	Sumter County, FL

Special Acknowledgements:
Delaine Arnold, ENP (dec.), and Sandy Dyre, ENP, Committee Resource Management, have facilitated the production of this document through the prescribed approval process. The Security Audit Checklist 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
- Brandon Abley, ENP, Chief Technology Officer
- April Heinze, ENP, VP, Chief of 9-1-1 Operations