

Table of Contents

1	Cybersecurity Objective.....	1
2	NPSBN Cybersecurity Concepts.....	1
2.1	Public Safety Needs.....	1
2.2	Dedicated Cybersecurity Program	2
2.3	Federal Requirements.....	2.1
2.4	Cybersecurity Architecture	3
2.4.1	Industry Best Practices.....	3
2.4.2	Devices and Applications	6
2.4.3	Application Security	7
2.4.4	Strong Identity, Credential, and Access Management	8
2.4.5	Cryptography	8
2.4.6	Public Safety Enterprise Network Security	9
2.5	Cybersecurity Life-Cycle Process.....	9
2.5.1	Identifying Vulnerabilities.....	9
2.5.2	Identifying Threats.....	9
2.5.3	Determining Risks Arising from Threats and Vulnerabilities	9
2.5.4	Prioritizing Risks to Determine Associated Controls	10
2.5.5	Specifying Controls to Address or Mitigate Threats and Vulnerabilities	10
2.5.6	Implementing Controls	10
2.5.7	Assessing the Effectiveness of Controls.....	10
2.5.8	Monitoring the Security of the System.....	10
2.6	Cybersecurity Guidance	10
2.7	Cybersecurity Systems Engineering.....	11
2.8	Cybersecurity Risk Management	12
2.9	Cybersecurity Incident Response and Security Operations Center	12
2.9.1	Cybersecurity Incident Response Team.....	12
2.9.2	Security Operations Center.....	13
2.10	Cybersecurity Continuous Monitoring and Mitigation Methodology	13
2.11	Cybersecurity Testing and Certification Plan	14
2.12	Cybersecurity Network Management and Configuration Management Policy	15
2.12.1	Network Management.....	15
2.12.2	Configuration Management	15
2.12.3	Vulnerability Management.....	15
2.12.4	Patch Management.....	15
2.12.5	Centralized Security Log Management.....	16
2.13	Environmental and Physical Security.....	16
2.14	Information Security and Data Sensitivity	17

1 Cybersecurity Objective

The cybersecurity solution implemented by the Contractor in connection with the contract with the First Responder Network Authority (FirstNet) must comply with the following provisions from the Middle Class Tax Relief and Job Creation Act of 2012 (the Act):

- Section 6206(b)(2)(A) requires FirstNet to “ensure the safety, security, and resiliency of the network, including requirements for protecting and monitoring the network to protect against cyberattack.”
- Section 6206(c)(2)(A)(iv) requires FirstNet to “consult with regional, State, tribal, and local jurisdictions regarding the distribution and expenditure of any amounts required to [establish network policies] with regard to the adequacy of hardening, security, reliability, and resiliency requirements.”
- Section 6203(c)(1)(A) required the Federal Communications Commission (FCC) to “develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the nationwide public safety broadband network [NPSBN].” On June 21, 2012, the FCC approved by Order (FCC 12-68) the Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network (Section J, Attachment J-3, FCC TAB RMTR) that was released on May 22, 2012, *as clarified* on June 6, 2012.
- The Act also requires FirstNet to comply with the Third Generation Partnership Project (3GPP) (Section 6001); Long Term Evolution (LTE) (Section 6203); and open, non-proprietary, commercially available standards (Section 6206(b)(2)(B)(i)).

FirstNet refers to the overall cybersecurity approach as the NPSBN cybersecurity solution. The concepts contained in this document are critical to the successful development, implementation, evolution, and maintenance of the NPSBN cybersecurity solution. The solution will be a joint effort of FirstNet and stakeholders involved with the NPSBN.

2 NPSBN Cybersecurity Concepts

The NPSBN cybersecurity solution should be based on the following minimum cybersecurity concepts to ensure the NPSBN is protected, operating with an acceptable level of risk, and accessible for public safety users. These concepts should be considered critical to the design of the NPSBN cybersecurity solution.

2.1 Public Safety Needs

The NPSBN cybersecurity solution should ensure that the NPSBN is protected from cyberattack but also ensure public safety users can readily access the network. All critical operational equipment and functions, which could affect the secure and effective operations of the NPSBN, shall be located within the sole jurisdiction of the United States. To that end, the solution should take into account the following areas:

- **Usability** – The network should be usable by Public Safety Entities (PSEs). Security controls, policies, and procedures should provide protection without impacting operability or interoperability.

- **Mission Primacy** – The mission of public safety—to protect lives and property from clear and present danger—should take primacy over protection of the network.
- **Operational Security** – The NPSBN cybersecurity solution should protect public safety users from situations where a security breach leads to an operational security breach.
- **First Responder Safety** – The NPSBN cybersecurity solution should not negatively affect first responder safety or impair requests for assistance in a responder emergency or immediate peril situation.
- **Reliability/Resiliency** – The NPSBN cybersecurity solution should enhance the reliability and resiliency of the NPSBN.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** – Traffic and transactions governed by HIPAA and subsequent related laws will transit and potentially be acted upon within the NPSBN.
- **Criminal Justice Information Services (CJIS)** – Traffic and transactions governed by the Federal Bureau of Investigation’s CJIS Security Policy will transit and potentially be acted upon within the NPSBN.
- **Payment Card Industry (PCI)** – Traffic and transactions requiring PCI compliance will transit the NPSBN.
- **End-to-End Encryption of User Communications and Data** – Public safety users expect their communications and data to be secure from end to end. Data loss prevention techniques should apply to all public safety data while at rest on the server/device, in transit, and in use. The NPSBN cybersecurity solution should encrypt user plane and signaling communications everywhere possible.
- **Privacy** – The privacy of the user and the user’s data is as important as its cybersecurity and should be accounted for.
- **Authentication** – Authentication methodologies on the network and for devices should allow public safety easy access but provide a high level of security. The solution should include federated Identity, Credential, and Access Management (ICAM) in concert with appropriate multifactor and step-up authentication approaches.
- **Multi-Layer Security** – It is critical that the NPSBN support layered security policies that permit PSEs to implement their unique security policies, provided that doing so does not compromise the overall security of the NPSBN. Inherently, a PSE security implementation, layered on top of the NPSBN, will only be interoperable to users authorized by the jurisdictional security authority.
- **Data Protection** – The protection of public safety data is critical for PSEs and first responders. The solution should prevent unauthorized disclosure (confidentiality), modification (integrity), or the inability to access the data when it is needed (availability).

2.2 Dedicated Cybersecurity Program

The NPSBN cybersecurity solution should include a dedicated cybersecurity program that considers all source threats; constructs a dynamic threat profile; generates a cybersecurity architecture; builds in proactive forensics; and establishes incident response capabilities that ensure the ability to operate and deliver crucial services as needed during a national, state, or local incident.

2.3 Federal Requirements

The NPSBN cybersecurity solution should enable all relevant entities to meet applicable federal cybersecurity standards and requirements, including any applicable requirements under the Federal Information Security Modernization Act of 2014 (FISMA).

2.4 Cybersecurity Architecture

To establish a secure NPSBN, the network architecture should, at a minimum, implement the recommended requirements listed in Section 1.3.7, Security, and the recommended considerations listed in Section 1.4.8, Security, of Section J, Attachment J-3, FCC TAB RMTR, as well as the following 3GPP specifications: TS23.401, TS33.102, TS33.210, TS33.310, TS33.401, and TS33.402.

2.4.1 Industry Best Practices

The NPSBN cybersecurity solution should implement industry best practices for wireless carriers, information technology, and critical infrastructure, including but not limited to the following areas:

- **Transport Security** – The solution should protect the S1 interface (between the base station and Core) and all other communications planes between Evolved Node Base stations (eNodeBs) and Core sites, including S1, X2, and all other management and timing plane communications between these devices.
- **Domain Security** – The solution should protect the end-to-end network by dividing it into domains, providing protection between domains, providing security policies and procedures for each domain, and protecting any inter-domain traffic as well as traffic transiting domains. Domains may include the following:
 - Radio Access Network within a state or territory
 - Backhaul network (eNodeB to regional aggregation points)
 - Aggregation network (aggregation of traffic in a region)
 - National transport networks (network connections to regional and national Core sites)
 - Evolved Packet Core (EPC)
 - Business support systems
 - Operational support systems
 - Applications ecosystem
 - Internet Protocol (IP) Multimedia Subsystem
 - Value-added services
 - Messaging services
 - Public Safety Enterprise Network (PSEN) connectivity
 - FirstNet cloud environments
- **External Interface Protection** – The solution should safeguard all external interfaces with appropriate security protections, such as firewalls, protection from common Internet attack vectors (e.g., Denial of Service [DOS], Distributed DOS [DDOS], spoofing, malware, botnets, port scanning), intrusion prevention and detection, security gateways, security logging, and content inspection/filtering. External interfaces may include:
 - SGi interface
 - Roaming interfaces such as S8 and S6a
 - Public Switched Telephone Network (PSTN) and Voice over IP (VoIP) peering for voice and messaging traffic
 - PSEN interfaces
 - Network partner, network element provider, and other third-party remote connection interfaces required for on-call or emergency maintenance and troubleshooting
 - Applications ecosystem interfaces with content providers, application developers, and service providers offering services via the applications ecosystem

- **End-to-End Security Management and Logging** – The solution should support a security information and event management (SIEM) solution to enable security analysis of large volumes of collected data and enable interfaces to the NPSBN for information sharing purposes. Further details are contained in Section 2.12, Cybersecurity Network Management and Configuration Management Policy.
- **Fraud Prevention and Revenue Assurance** – The solution should include fraud prevention and revenue assurance functionalities to ensure that resources are being used appropriately and charging and service control transactions are providing a true picture of network usage.
- **Network Address Translation** – The solution should implement network address translation and other associated functions for end-user traffic. Where required, static addressing should be made available as well.
- **Protection Between Users** – Where appropriate, and not at the expense of operability, the solution should protect users from other users on the network. There are times when direct device-to-device communications through the network are required, such as user plane communication during an IP Multimedia Subsystem session, but attack vectors such as a ping of death, port scanning, and DOS should be prevented between end users.
- **Signaling Storms** – The solution should detect and prevent signaling storms both inside the network and on external signaling interfaces. This may be accomplished with Diameter Routing Agents and proxies.
- **Rogue or Stolen Devices** – The solution should protect against rogue devices and/or stolen devices (e.g., devices deemed an operability or security risk, devices that have been compromised, or devices that have not successfully passed device certification processes). The solution may include Equipment Identity Register functionality but should also include detection functionality. A device or class of devices should be able to be blacklisted/un-blacklisted either manually or automatically. Automatic blacklisting must not jeopardize the safety mission of first responders.
- **Heterogeneous Networks** – The solution should enable small cells and heterogeneous networks, potentially offered by a third party, to securely authenticate and interconnect to the Core network.
- **Operational Support System** – The solution should include an operational support system that implements FCAPS (fault management, configuration management, accounting management, performance management, and security management), authenticates all users connecting to network elements for maintenance and operations, and logs all access and configuration actions. Further details are contained in Section 2.12, Cybersecurity Network Management and Configuration Management Policy.
- **Domain Name Service (DNS) Security** – The solution should deploy a secure DNS solution and distinct DNS domains/zones for Transport Security, the evolved packet core, the roaming network, and the SGi interface. These domains/zones should be completely separate and distinct.
- **Messaging Security** – The solution should include a messaging security solution that protects the messaging infrastructure as well as the attack vectors within the messages themselves. This may include anti-virus, anti-spam, and malware protection as well as IP-reputation verification. Messaging may include email, instant messaging, short messaging, and multimedia messaging.
- **IP Multimedia Subsystem Security** – The solution should include an IP Multimedia Subsystem security solution that protects it from an infrastructure, signaling, and user-plane prospective.
- **Business Support Systems Security** – The business support systems should include but not be limited to mediation, charging, billing, provisioning, local control, and customer relationship

management. These systems should be protected and include access control and full transactional logging.

- **Mobile Virtual Private Networks (mVPNs)** – The solution should enable an mVPN solution to ensure PSEs can securely communicate and still utilize Quality of Service, Priority, and Preemption. If secure communications are required by public safety for network services such as messaging, NPSBN cloud services, or IP Multimedia Subsystem, then mVPNs should be able to be terminated inside the Core network.
- **Business Continuity Planning, Disaster Recovery Planning, and Crisis Management** – The solution should utilize industry best practices for business continuity planning, disaster recovery planning, and crisis management.
- **IP Infrastructure Network Elements** – The solution should ensure all routing and switching network elements are hardened and configured to only allow traffic that is required to transit the network using access control lists and other methodologies.
- **Security Hardening** – All network elements should be hardened according to defined policy, process, and guidelines and should be continuously monitored for compliance. Specifically, security hardening should include:
 - Patch maintenance
 - A security hardening tool portfolio
 - Access control, including the associated system configuration and policy
 - File system hardening and access control
 - Network security
 - Process security
 - Host logging
 - Time synchronization
- **Cybersecurity Governance Model** – The cybersecurity governance model should include a security governance organization; security governance policies; security functional requirements; security risk identification, analysis, and mitigation; security technical controls; security operational controls and procedures; security responsibilities and practices; strategies and objectives for security; risk assessment and management; and resource management for security.
- **Supply Chain Cybersecurity** – The solution should ensure the cybersecurity of the supply chain throughout the life of the contract is verifiable and that no vulnerabilities, exploits, or threat vectors have been introduced to products prior to installation in the NPSBN.
- **Training** – Human factors within cybersecurity are considered as one of the most important but most difficult areas to assess and protect. The solution should provide training for users and operators to increase the cybersecurity of the NPSBN.
- **Insider Threat Mitigation** – The NPSBN cybersecurity solution should include prevention, control, mitigation, and detection of insider threats.
- **Cloud Security** – There should be a robust cybersecurity solution for any cloud services offered within the NPSBN. The cloud security solution should provide identity management tied to that of the NPSBN, physical security, personnel security, availability, application security, and privacy.
- **Virtualization Security** – As virtualization becomes more common, even within the EPC through Telco Cloud and network-functions virtualization, the cybersecurity of the virtual environment requires additional focus to ensure there are no cyber risks introduced to the network through virtualization.
- **VoIP Spam** – The solution should mitigate VoIP spam, or Spam over Internet Telephony, as well as “robo dialing.”

2.4.2 Devices and Applications

To ensure the security of User Equipment (UE) and devices, the NPSBN cybersecurity solution should include but is not limited to the following elements:

- **Secure Operating System Architecture**
 - Boot loaders, which initiate the operating system (OS) of the device, should not be allowed to be tampered with by malware. OS vendors now take on the responsibility of building bootloaders into their software instead of employing third-party software.
 - [bullet removed]
 - The secured container solution should be used to protect agency applications and user data in mobile devices. Security policy guidelines and processes should be used for secured container solution in protecting agency data with a user's personal application.
 - Devices should be continuously monitored both online and offline to ensure the OS is not compromised and that devices have not been "jail broken" or "rooted."
 - FirstNet and its selected Contractor will work with device manufacturers on OS updates related to security issues and local control Mobile Device Management (MDM) solutions to enable PSEs to provide updates to public safety users.
 - The device local storage must be encrypted with OS capability.
- **Authentication of Users and Applications**
 - MDM should enable the PSE administrator to enforce device and application password policies remotely.
 - MDM should enable authentication for access to the collection of secured applications on the device.
 - Certificate or token-based authentication of certified applications should be available.
 - Device-specific biometric authentication (e.g., fingerprint, retina) should be integrated for supplemental authentication of certified access to the application.
- **Embedded Applications**
 - Latency-sensitive mission-critical applications (such as Mission-Critical Push-to-Talk) should be signed and certified (validated as prescribed by FirstNet) and should be provided to various Original Equipment Manufacturers as part of pre-installed applications on the device.
 - Internal embedded clients should use non-exposed Access Point Names (APNs) for access all certified applications or for PSE network access.
- **MDM and Mobile Application Management (MAM) – PSE-Managed Whitelist/Blacklist**
 - The PSE administrator should be able to wipe or lock a lost or stolen device.
 - The PSE administrator should be able to manage applications on devices through MDM.
- **Digital Signature of the Applications** – Digital signatures of FirstNet and partners' signed applications should be verified by the device.
- **Device Security Solutions** – Device security solutions should be provided, including smartphone/device security that includes anti-virus; firewall; remote management of applications and services; monitoring; theft prevention; device access control; and protection of the UE by the network with content inspection/filtering, messaging security, and the protections provided through other methodologies in this section.
- **Bring Your Own Stuff** – Cybersecurity solutions should address Bring Your Own (Device, Application, or Wearable) approaches.

2.4.3 Application Security

To ensure the security of applications, the NPSBN cybersecurity solution should include but is not limited to the following elements:

- **Applications Ecosystem Security** – The solution should provide protection for the NPSBN applications ecosystem, including the associated applications store, application development environment, cloud services, Service Delivery Platform (SDP), Application Programming Interface (API), applications, and the PSE networks. The Offeror-provided public safety applications and data, local control, and agency home page portal need to be secured and protected against all threats, including external threats, internal threats, data breaches, and DOS attacks.
- **API Security** – The Contractor will develop new NPSBN capabilities and services and expose specific APIs to enable new applications. These APIs, services, and applications will allow for new capabilities such as dynamic control of Quality of Service, priority, preemption, local control, agency home page status, and public safety analytics. APIs give developers—both legitimate developers and potential system hackers—more finely grained access into an application than a typical Web application. The solution should address API threats, including but not limited to the following:
 - Parameter attacks that exploit the data sent into an API, including URL, query parameters, HTTP headers, and/or posted content
 - Identity attacks that exploit authentication, authorization, and session tracking
 - Man-in-the-middle attacks that intercept legitimate transactions and exploit unsigned and/or unencrypted data
 - Protection of sensitive APIs from unauthorized use
- **Application Audit** – Proper logging and auditing can provide invaluable information and uncover more than just security concerns. The solution should ensure applications properly log and audit the actions by the user and information about the user who takes those actions.
- **Application Security in Software Development Life-Cycle** – The solution should promote secure programming and provide developers with tools to ensure they keep security in mind throughout the software development process. Currently, there are several code analysis and test tools available commercially or through open source.
- **Application Security Certification** – The solution should ensure the NPSBN’s application security and certification process includes analyzing the application both statically and dynamically for security vulnerabilities. Making these tools and methods available to developers in order to catch vulnerabilities and potential risks as early as possible in the development life-cycle is critical. Such tools and assessments should be continually used, even after an application has been certified, because the security landscape changes with new risks and vulnerabilities discovered daily. The solution should ensure all mobile, Web, and desktop applications published on the NPSBN applications store (also referred to as the “FirstNet applications store”) undergo a defined certification process to ensure usability, reliability, privacy, security, and safety. This process should allow PSEs to have a high degree of confidence when downloading or purchasing certified applications from the NPSBN applications store.
- **Application Developer Certification** – The application developers registering with the NPSBN and publishing the applications should be audited and certified apart from the applications.
- **User Logging** – The solution should ensure administrators and users accessing the application ecosystem are logged audited and transactions are recorded. Proper logging and auditing can provide invaluable information and uncover more than just security concerns.

- **End-to-End Application Analysis** – The solution should leverage a log analysis tool to analyze application, Core, network, and other log files. There are several advanced tools available that allow for real-time analysis and generate alerts based on events detected by analyzing log files and other information feeds. These can provide the Security Operations Center with detailed views into the behavior of the applications ecosystem and provide vital security reports and information.
- **Validation of Application-Specific Port Monitoring** – Any non-standard ports used by an application need to be monitored for any security breach.
- **Application Protection** – The solution should provide protections to ensure only approved applications are loaded and run on a UE.
- **Application-Device Security** – The solution should provide protections to ensure applications cannot bypass OS security on devices.
- **Data Loss Prevention** – The solution should provide protections to ensure applications protect data while at rest, in use, and in transit.
- **Secure Application Coexistence** – The solution should provide a secure method of coexistence among NPSBN-certified applications and commercially available applications on a device.

2.4.4 Strong Identity, Credential, and Access Management

To ensure the security of user identities, the NPSBN cybersecurity solution should include but is not limited to the following elements:

- **ICAM** – The solution should support federated identity from PSE networks.
- **Identity Assurance** – The solution should ensure the following relationships are authenticated:
 - User to Device – PSEs may not acquire one device for every user. It therefore becomes critical to know which first responder has the device.
 - Device to Network – LTE authentication
 - Network to Application – Identity management
 - Network to PSE Network – Identity management
 - User to Application – Identity management
 - User to PSE Network – Identity management
- **Authorization** – The solution should ensure users are properly authorized to access applications, data, and services through the use of Attribute Based Access Controls (ABAC), Policy-Based Access Controls (PBAC), and similar methods.
- **Credentialing** – The solution should ensure that agencies are following the process for identity proofing users and assigning credentials.
- **Auditing** – The solution should ensure that all user actions are properly monitored and audited.

2.4.5 Cryptography

LTE is designed with strong cryptographic techniques, mutual authentication between LTE network elements, and security mechanisms built into its architecture. With the emergence of the open, all IP-based, distributed architecture of LTE, attackers can target mobile devices and networks with spam, eavesdropping, malware, IP-spoofing, data and service theft, DDOS attacks, and numerous other variants of cyberattacks and crimes. This will necessitate appropriate safeguards and mitigation approaches to negate the impact of these attack vectors.

2.4.6 Public Safety Enterprise Network Security

The NPSBN cybersecurity solution should recommend minimum security standards for state and local agencies. The solution should include initiatives to educate state and local agencies on cybersecurity topics related to the NPSBN and to review and advise agencies on strengthening their security architectures and policies, if needed, prior to connecting to the NPSBN.

2.5 Cybersecurity Life-Cycle Process

The NPSBN cybersecurity solution should include an ongoing cybersecurity life-cycle process that employs and monitors security controls, ensuring continued viability and effectiveness of the NPSBN. The primary areas of this process include the following, which are performed in a recurring cycle over time as older threats and vulnerabilities become negated and new ones arise:

- Identifying vulnerabilities
- Identifying threats
- Determining risks arising from threats and vulnerabilities
- Prioritizing risks to determine associated controls
- Specifying controls to address or mitigate threats and vulnerabilities
- Implementing controls
- Assessing the effectiveness of controls
- Monitoring the security of the system

Key to this ongoing approach will be 3GPP feature enhancements and major release upgrades being made available and implemented on the NPSBN. The solution should include a plan to address associated support for security upgrades to network infrastructure and devices as capabilities advance generationally. The solution should include provisions to establish security support for aging network infrastructure and devices and sunset procedures for network infrastructure and devices when they are no longer viable.

2.5.1 Identifying Vulnerabilities

Vulnerabilities can surface in virtually all aspects of the NPSBN enterprise. It is critical to be aware and capable of identifying those vulnerabilities present in software (e.g., OSs, applications, protocols, encryption), hardware, firmware, and related capabilities. Vulnerabilities will need to be documented appropriately to permit development of suitable controls as well as determine the effectiveness of those controls.

2.5.2 Identifying Threats

Threats can take multiple forms and provide attack vectors to all components of the NPSBN enterprise. The Core network, Radio Access Network, UE, applications, and backhaul transport are subject to a range of threats. The threats will need to be documented appropriately to permit the development of suitable controls as well as determine the effectiveness of those controls.

2.5.3 Determining Risks Arising from Threats and Vulnerabilities

Once the relevant threats and vulnerabilities have been identified and documented, it will be necessary to determine the risks tied to each. In some cases, the risk will be sufficiently improbable as to not require any action. For all others, an impact determination will be accomplished to rank where the risk falls relative to other risks.

2.5.4 Prioritizing Risks to Determine Associated Controls

After risks have been assigned respective impact determinations, they will be ranked in order of criticality to determine mitigation. Risks that have no direct correlation to an internally controlled mechanism will be either accepted or transferred (e.g., through procurement of insurance against the risk). Those risks tied to a particular vulnerability or threat will be evaluated based on impact and viability of mitigation. Upon final ranking and evaluation, appropriate controls will be addressed.

2.5.5 Specifying Controls to Address or Mitigate Threats and Vulnerabilities

Once the threats and vulnerabilities have been identified and prioritized, suitable controls will be identified to mitigate them. In the event, there is no viable control to address a threat or vulnerability, a determination of acceptance of risk and a proposed fix should be documented and provided. Revalidation should occur periodically, but no less than quarterly, to determine if the proposed fix is available and if the current acceptance is still sufficient.

2.5.6 Implementing Controls

All selected and specified controls will be implemented prior to Initial Operational Capability when possible; those controls developed subsequently or as new controls supersede existing solutions will be implemented as quickly as possible but not before ensuring they do not introduce unanticipated problems elsewhere. Implementation of controls will adhere to the guidance found in Section 2.12, Cybersecurity Network Management and Configuration Management Policy.

2.5.7 Assessing the Effectiveness of Controls

After implementation, the effectiveness of the specified controls will be assessed on an ongoing basis to ensure they perform their function as expected. The results of the ongoing assessment will be documented appropriately and retained for situational awareness.

2.5.8 Monitoring the Security of the System

The NPSBN will be monitored for performance and security and security control indicators will be tracked to determine their effectiveness against identified threats. Monitoring will also be used to develop awareness of new threats and begin the cybersecurity life-cycle process again, if needed. The process is iterative and does not end as new threats and the need for associated security controls continues indefinitely.

2.6 Cybersecurity Guidance

There is considerable cybersecurity guidance available from industry, government, and standards organizations that should be considered when developing the NPSBN cybersecurity solution. There is no single solution or guidance that addresses all cybersecurity challenges. When considering the complexity of the NPSBN and the fact that its components, users, and usage falls into many different cybersecurity areas of practice, the NPSBN cybersecurity solution should employ multiple frameworks to address these needs.

2.7 Cybersecurity Systems Engineering

The NPSBN cybersecurity solution should take into account the best practices of systems engineering but expand them with the best practices of cybersecurity engineering. Cybersecurity systems engineering should:

- Include a cybersecurity systems engineering plan that enumerates operational policies and procedures at all levels.
- Include a repeatable process that is executed continuously both during the development and evolution of the NPSBN.
- Ensure cybersecurity engineering is considered in all decisions, designs, and actions related to the NPSBN. The network should meet the core tenets of cybersecurity for a modern, robust wireless communications system while following the principles of systems engineering, including documented and robust use of the people, processes, and technology required to provide security with minimal impact to the user population.
- Maintain the simple, overarching cybersecurity principles of the NPSBN:
 - Ensure the network is being used by only the authorized personnel it supports
 - Ensure the network and its users are protected from all others, whether they are external adversaries or insider threats
 - Ensure the cybersecurity program is robust and capable of detecting if any of the cybersecurity principles are not true
- Ensure the cybersecurity design of the network and components:
 - Plans, develops, and tests new technologies
 - Performs technical analysis in support of development and test activities for new systems and emerging technologies
 - Facilitates the development of future requirements and architecture components to enable the transition of new systems and technologies into the operational baseline
 - Coordinates future technology efforts with internal and external partners and operational users
- Facilitate cybersecurity assessment, including but not limited to:
 - Utilizing a third-party, independent organization to provide laboratory and field security assessments
 - Performing independent verification of NPSBN planning and infrastructure
 - Adopting best practices from other federal agencies and industry
 - Running large-scale scheduled cybersecurity exercises and targeted local cybersecurity exercises as needed
- Utilize resilient design principles, including but not limited to:
 - Engineering a resilient network. This requires balancing single points of failure and economics
 - Aligning with 3GPP Release 9 LTE, which introduces IP as the basic connectivity between network elements.
 - Securing the NPSBN's network architecture, which will ensure that single points of failure are reduced as low as economically reasonable. The impact of single points of failure can be reduced by utilizing:
 - Self-Organizing Networks
 - Site hardening (physical security)

- Layers of network coverage
- Industry best practices to protect against systemic failures, cyberattacks, and human errors
- Establish application security policies and procedures that encompass distribution of applications that can be used on the NPSBN.

2.8 Cybersecurity Risk Management

The NPSBN cybersecurity solution should have a detailed and robust risk management methodology that is executed continuously during the system's development life-cycle and during the life of the program and the NPSBN.

The risk management methodology should, at a minimum, contain the following steps:

- Asset identification
- Risk impact analysis
- Threat assessment
- Risk mitigation
- Security control selection and deployment
- Risk mitigation operations and maintenance

The methodology could be based on or enhanced by existing models, such as the National Institute of Standards and Technology (NIST) Risk Management Framework or the ISO 27000 series.

2.9 Cybersecurity Incident Response and Security Operations Center

The NPSBN cybersecurity solution should address incident reporting and response, which are critical to the security of the NPSBN. If an incident or event is deemed to require travel to a site for additional security investigation and analysis, the Government will require the Contractor to dispatch staff within a time period to be established, but potentially in as little time as one business day.

2.9.1 Cybersecurity Incident Response Team

The NPSBN cybersecurity solution should account for a Cybersecurity Incident Response Team that will be responsible for managing incident response. At a minimum, the team should perform the following activities:

- Coordinate the notification and distribution of an incident
- Mitigate the risk of an incident by minimizing disruptions
- Notify the contracting officer if it appears that the mitigation will have an associated cost
- Assemble security staff to conduct a threat assessment and resolve the incident
- Take reasonable steps to mitigate the effects and to minimize any damage resulting from the incident
- Monitor system logs for application to the incident
- Categorize all security incidents per policies and procedures and report them within specific time frames, to be identified
- Define and capture metrics that will be used for reporting

- Provide a post-mortem for each incident associated with an actual cyberattack in a format agreed upon by the Contractor and FirstNet
- Provide an after action report for any incident that occurs due to inadvertent actions by authorized operations and maintenance personnel in a format agreed upon by the Contractor and FirstNet
- Record or log all security incidents in an electronic format (to be determined). These logs will provide the information for reporting purposes
- Report all security incidents based on incident severity, as directed in standard operating procedures that will be developed jointly between the Contractor and FirstNet

All incidents must be immediately reported, whether suspected or confirmed, including potential risks to the confidentiality, integrity, or availability of NPSBN information or to the function of NPSBN systems.

Upon becoming aware of any unlawful access to data or information stored on the Contractor's equipment or in the Contractor's facilities, or unauthorized access to such facilities or equipment resulting in the loss, disclosure, or alteration of any FirstNet data or information (a "Security Incident"), the Contractor should notify the Contracting Officer immediately.

2.9.2 Security Operations Center

The NPSBN cybersecurity solution should include a Security Operations Center that provides:

- Situational awareness, including collecting, maintaining, and sharing information about threats to network infrastructure, devices, data, and applications
- 24/7/365 cybersecurity monitoring of Core network infrastructure, devices, data, and applications
- Monitoring and analysis of user, system, and network access
- Assessment of the integrity of the system and data files
- Establishment of the baseline network activity and utilization to use as a reference
- Recognition and analysis of activity patterns that are indicative of an incident or intrusion
- Analysis of logs for abnormal use patterns
- Information sharing and collaboration that integrates and disseminates information throughout the critical infrastructure partnership network
- Processing and posting suspicious activity reports
- Assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications
- Decision support that provides recommendations to partners and FirstNet leadership

2.10 Cybersecurity Continuous Monitoring and Mitigation Methodology

The NPSBN cybersecurity solution should include a cybersecurity continuous monitoring approach and mitigation methodology that addresses the following elements:

- Continuous Monitoring and Forensics – The solution should adopt active security tools and solutions that continuously monitor, log, and provide forensic data about the current state of the network and any changes that have occurred.

- The solution should support a continuous monitoring approach that includes the following components and processes:
 - Hardware Asset Management – the automated means of tracking which components are on the network and their associated attributes. This ensures awareness of what systems are operating and that they are legitimate components.
 - Software Asset Management – the automated means of tracking software running on the network and ensuring consistent versions and releases are the only ones permitted to run and those failing the mark are upgraded or removed.
 - Vulnerability Management – entails scanning software throughout the network as well as traffic traversing the network for signatures or behavior that are atypical. Items identified in vulnerability scans are then referred for analysis and further investigation.
 - Configuration Settings Management – deals with settings on network components, such as router access control lists or firewall settings. An automated toolset evaluates settings against baseline standards to ensure consistency of configuration as well as ensuring simple typos do not result in compromising the network.
- Mitigation of identified issues from continuous monitoring takes multiple forms and is dependent on the nature of the specific issue. For example, determining if misconfigured hardware is updated with the correct settings requires different mitigation solutions than ensuring out-of-date software is patched and/or replaced.

2.11 Cybersecurity Testing and Certification Plan

The NPSBN cybersecurity solution should include a testing and certification plan that is tailored to cybersecurity issues. The plan should, at a minimum, address the following areas:

- **Testing Life-cycle** – Processes should be established to verify security approaches through a life-cycle of selection, procurement, integration, and operations support. This is often a key functionality within an organization’s greater cybersecurity systems engineering practice. The testing methods will include assessment, testing, examination, and interviewing. All testing results should be retained to provide baseline standards for ongoing testing to ensure optimal accuracy and reproducibility.
 - Assessment is the process whereby a security control is evaluated as to how well it meets stated security objectives.
 - Testing is the subjection of the security control to inputs to determine what results occur.
 - Examination is the review of related documentation for one or more controls to determine stated objectives and capabilities.
 - Interviewing is the discussion with designers, implementers, and users regarding the expectations and behaviors of the stated controls on the system.
- **Individual System Validation** – Individual systems should be validated by an independent assessor in a continuous improvement and feedback fashion to maximize the depth and value of the assessment, as well as to test the responsiveness to the process.
- **Integrated Configuration Testing** – Pilots for user functionality enable successful full-scale security scanning, assessment, and testing for new vulnerabilities introduced as part of the fielding process, as well as testing of initial security monitoring, intrusion detection, and cyber incident response capabilities.

- **Independent Applications/Services Testing** – All applications that are distributed by the Core network or exchange data with the Core network should undergo formal testing, validation, and authentication prior to distribution to provide reasonable assurance of their respective security posture. For evolving integration with PSE networks, the security policies and posture can be determined by application data flows (local vs. national) and the use of distinct gateways that can defend those boundaries. Testing and validation should address applications for each of the following situations, as appropriate in the life-cycle of the application as well as its origination:
 - New applications at the national level
 - User-developed or state-developed applications
 - Upgrades to currently approved applications
 - Security patches to currently approved and fielded applications

2.12 Cybersecurity Network Management and Configuration Management Policy

The NPSBN cybersecurity solution should include policies for network management and configuration management.

2.12.1 Network Management

The NPSBN cybersecurity solution should involve the management and maintenance of cybersecurity tools and capabilities by an out-of-band network that limits access to devices to a small number of authorized personnel. If this is not practical, then alternative methods, such as a Virtual Private Network (VPN), should be employed.

2.12.2 Configuration Management

In the context of cybersecurity, configuration management is the practice of handling changes to security tools, software, and devices in a repeatable, systemic manner to ensure the security and the integrity of the security processes over time. Configuration management will be developed and implemented to ensure cohesive policies, procedures, techniques, and tools to manage, evaluate a proposed change, track the status of implementation of any approved changes, and maintain the artifacts of system and support documents as they change. From the American National Standards Institute/Electronic Industries Alliance standard 649, the five distinct disciplines should be:

- Configuration Management Planning and Management
- Configuration Identification
- Configuration Control
- Configuration Status and Accounting
- Configuration Verification and Audit

2.12.3 Vulnerability Management

The NPSBN cybersecurity solution should include a methodology to conduct and maintain routine, consistent vulnerability scanning of NPSBN infrastructure that is passive in nature to ensure no impact to systems. Any discovered vulnerabilities should result in efficient, effective remediation.

2.12.4 Patch Management

The NPSBN cybersecurity solution should establish a continuous cycle of applying software updates and patches for all software provided with the system, including OSs and third-party applications. Patches

should be thoroughly vetted through a verification and validation lab. This will provide NPSBN users and leadership assurance that the patch updates will not negatively impact the operational capabilities of the wireless communications system. A critical aspect of a patch management solution for wireless communications systems is the ability to test critical vulnerabilities out of cycle, which cannot wait until the next scheduled patch distribution.

The solution should adhere to industry best practices for a patch management solution, including:

- Centralized, role-based administration
- Integration with an authentication and authorization server
- Patch scheduling and administration
- Air-gap patches capability, which requires updating the patch management server with mobile media (e.g., DVD or thumb drive) without connectivity to the Internet required

2.12.5 Centralized Security Log Management

The NPSBN cybersecurity solution should include SIEM—a tool focused on the security aspects of log management, which involves collecting, monitoring, and analyzing security-related data from computer logs. Security-related data includes log data generated from numerous sources, including antivirus software, intrusion detection systems, file systems, firewalls, routers and switches, and servers. SIEM is responsible for the aggregation and normalization of security-related data and allows for analysis on a large number of logs in an efficient manner.

2.13 Environmental and Physical Security

Environmental and physical security is critical to security planning for any information systems. This capability is one of the most mature tenets of security. However, because the NPSBN will be disparately deployed across the nation, environmental and physical security can quickly become cost-prohibitive. Environmental and physical security systems should be capable of monitoring alarms, centrally displaying and reporting the alarm status of the entire system and all sub-components, and forwarding critical alarm notifications to appropriate personnel within the Network Operations Center or Security Operations Center.

The NPSBN cybersecurity solution should take into consideration the following physical and environmental security elements:

- Power Failure
- Humidity Detection
- Cabinet Door Alarms
- Uninterruptable Power Supply Power Failure
- Access Control to and Within a Facility
- Monitoring and Recording of Activity Within a Facility to Include Egress/Ingress
- Movement Activity Within a Facility After Hours or in Restricted Areas
- Heating, Ventilation, and Air Conditioning (HVAC) Failure or Degradation
- Building Door Alarms
- Generator Failure
- Low Generator Fuel
- Low Battery
- Closed Circuit Television (CCTV) Video Surveillance Systems

-
- Fire/Smoke Detection Sensors
 - Protection from Natural Disasters (e.g., lightning/surge protection, water leak detection)

2.14 Information Security and Data Sensitivity

All data in transit, accessed, or stored across the NPSBN environment will be encrypted and handled as restricted data. The use, dissemination of, and access to restricted data are limited to specific agencies, individuals, and situations. Where existing data repositories employed by NPSBN users already have established levels of mandated sensitivity and protection, those levels should be used at a minimum. Retention of any data will be in accordance with agency record retention policy as specified by the respective data owner. Upon expiration of the retention period, data should be destroyed or otherwise disposed per agency policy. Data in the NPSBN should not be releasable to any external parties without compliance with applicable laws.