Appendix C-10
NPSBN
Cyber Security

Nationwide Public Safety Broadband Network (NPSBN)

10/5/2015

Table of Contents

1 Introduction

The Nationwide Public Safety Broadband Network (NPSBN) will be unique. FirstNet intends to include a diverse multi-platform user equipment base, more than 60,000 public safety enterprise (PSE) networks, more than 6,800 public safety answering points, a nationwide core network, an applications ecosystem, and a host of radio access networks spanning 56 states and territories. Due to the network's complexity, the design, deployment, and ongoing operations of the NPSBN will present unique cyber security challenges. FirstNet seeks cyber security solutions that match the unique and complex nature of the NPSBN's undertaking.

Traditional cyber security approaches tend to focus on local and enterprise fixed networks that are connected via physical fiber or cable with the majority of processing and access conducted from fixed locations. While wireless access has become more common, it still only represents a small sub-set of the central network. Moreover, traditional cyber security efforts rely heavily on established, accepted measures of regulation that emphasize compliance rather than actual security. The NPSBN, however, will require a different approach because a simple adoption of today's standards will not provide the level of mitigation or hardening against cyber threats required by FirstNet and its users. This call for a new approach was recently emphasized by several high-profile breaches of both industry and federal government systems, including the widespread compromise of the Office of Personnel Management in which personal information of more than 21.5 million current and former federal employees was stolen; the breach of United Airlines reservation and ticketing systems which revealed traffic patterns of origination and destination for millions of people; the email compromise of Sony Corporation; the hacking incident of the Census Bureau; and the cyber break-in of the USIS (United States Investigative Services), which handles background investigations for federal employee security clearances. In each of these scenarios, several common threads emerge:

1. An assumption there is no problem because documentation states the system(s) are in compliance therefore they are secure
2. Nonexistent monitoring of anomalous activity on the network, e.g., large amounts of data being sent outside of the normal network boundary
3. Lack of a baseline to indicate normal traffic and user behavior on the network
4. Lack of a regular review schedule of database access to determine if activity is valid

These are common issues in the compliance driven world of the Federal Information Security Management Act (FISMA) and its commercial equivalents. Traditional guidance doesn't focus on actual security but rather the generation of detailed reports. The burdensome nature of this approach drains thousands of man-hours from organizations yet fails to address in a systematic or holistic view the real cyber security concerns of the owning organizations. An example of this methodology lies in how continuity of operations COOP plans are validated to be in compliance. In reality, one would expect to test if the plan works by executing it and determining what does and does not work. FISMA allows one to perform a desktop certification to meet requirements. In other words, the organization reads what they wrote and then determines if it would work or not without actually verifying it in operation. A large number of these problems, which the compliance-driven model further exacerbates, involve layering security onto systems or networks after they are already operational. Security needs to be functionally and operationally focused in order to be effective and responsive. This can only be

achieved if security is intrinsic to the design and implementation of every aspect of the network and data environment from inception. This is the goal and approach to be employed by FirstNet.

Public safety users have two needs that often compete with each other. They must have instantaneous communications and the communications must be secure. A cyber security solution that establishes a secure network at the cost of delays or needless hindrances is not workable, and neither is a solution that permits immediate access but fails to adequately secure data. FirstNet seeks cyber security approaches that will prioritize effectiveness while ensuring that communications are not hampered. Thus, FirstNet's NPSBN cyber security efforts will be guided by three key principles: confidentiality, integrity, and availability. The NPSBN must be able to address cyber security from an end-to-end perspective within a changing geographic and mission base while also addressing routine and urgent operational needs for public safety entities.

Any cyber security solution adopted by FirstNet must also comply with the provisions of the Middle Class Tax Relief and Job Creation Act of 2012 (Act):

- Specifically, Section 6206(b)(2)(A) of the Act 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) of the Act 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) of the Act required the Federal Communications Commission (FCC) to develop minimum technical requirements to ensure a nationwide level of interoperability for the 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 (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)).

We refer to our overall cyber security approach as the NPSBN Cyber Security Solution. The concepts contained in this document are critical to the successful development, implementation, evolution and maintenance of the NPSBN Cyber Security Solution. The Solution will be a joint effort of FirstNet and contractor(s) involved with the NPSBN. Additionally, outreach to the states regarding the NPSBN Cyber Security Solution will contribute to FirstNet's already robust consultation efforts.

The cyber security challenges inherent in the development, deployment and operation of the NPSBN require a paradigm shift in how a network of this type is secured and defended. FirstNet seeks to create this paradigm shift so that the NPSBN can be appropriately defended.

2 NPSBN Cyber Security Concepts

The NPSBN Cyber Security Solution should be based on the following minimum cyber security concepts to ensure that the NPSBN is protected, operating with an acceptable level of risk, and usable for public safety users. Although some of the language in these concepts emphasizes their importance, these concepts are not requirements. Rather, they should be considered concepts that are important to the design of the NPSBN Cyber Security Solution.

2.1 Cyber Security Key Concepts

1. Public Safety Needs – It is the objective of FirstNet to ensure that the network is protected from cyber attack but not at the expense of public safety users' ability to use the network.
   a. Usability – It is essential that the network be usable by public safety entities. Security controls, policy and procedure should provide protection but not prevent operability or interoperability.
   b. Mission Primacy – It is essential that the mission of public safety—the protection of lives and property from clear and present danger—takes primacy over protection of the network.
   c. Operational Security – It is essential that the NPSBN Cyber Security Solution protects public safety users from situations where the breach of that security leads to the breach of operational security. The identity and role of first responders needs to be protected before, during, and after mission critical incident response.
   d. Responder Safety – It is essential that the NPSBN Cyber Security Solution does not negatively affect responder safety or impair requests for assistance in a responder emergency or immediate peril situation.
   e. Reliability/Resiliency – It is essential that the NPSBN Cyber Security Solution enhance the reliability and resiliency of the NPSBN.
   f. Health Insurance Portability and Accountability Act of 1996 (HIPAA) – It is expected that traffic and transactions governed by HIPAA and subsequent related laws will transit and potentially be acted upon within the NPSBN.
   g. Criminal Justice Information System (CJIS) – It is expected that traffic and transactions governed by CJIS Security Policy will transit and potentially be acted upon within the NPSBN.
   h. Payment Card Industry (PCI) – It is expected that traffic and transactions requiring PCI compliance will transit the NPSBN.
   i. End-to-End Encryption of User Communications and Data – Public safety users have the expectation that their communications and data are 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 Cyber Security Solution should encrypt user-plane and signaling communications everywhere possible.
   j. Privacy – Although cyber security is critical, the privacy of the user and the user's data is as important as its cyber security.
   k. 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 a federated Identity, Credential, and Access Management (ICAM) solution in concert with appropriate multifactor approaches to authentication.
   l. Multi-Layer Security – It is critical that the NPSBN support layered security policies that permit PSE jurisdictions to implement their unique security policies, provided that doing so does not compromise the overall security of the NPSBN. Inherently, a jurisdictional security

implementation, layered on top of the NPSBN, will only be interoperable to users authorized by the jurisdictional security authority.

m. Data Protection – The protection of public safety data is critical for the PSE and to the first responders, including protection from unauthorized disclosure (confidentiality), modification (integrity) or the inability to access the data when it is needed (availability).

2. Dedicated Cyber Security Program – This program should be capable of considering all source threats; crafting a dynamic threat profile; generating a cyber security architecture; building in proactive forensics; and establishing incident response capabilities that ensure the ability to operate, and deliver crucial services as needed in the midst of a national, state, or local emergency response situation.
3. Federal Requirements – The NSPBN will support federal users, therefore the NPSBN Cyber Security Solution should enable federal users to meet their cyber security requirements, including FISMA and other federal cyber security requirements.

2.2 Cyber Security Architecture

1. The NPSBN Cyber Security Solutions should, at a minimum, to implement the minimum requirements listed in Section 1.3.7, the recommended considerations listed in 1.4.8 of the FCC TAB RMTR, and 3GPP specifications TS23.401, TS33.102, TS33.210, TS33.310, TS33.401, and TS33.402.
2. Additionally, it is the objective of FirstNet to implement industry best practices for wireless carriers, information technology, and critical infrastructure in order to provide cyber security protection for the NPSBN. These best practices should include, but are not limited to:
    a. Transport Security – Protect the S1 Interface (between the base station and core) and all other communications planes between Evolved Node Bs (eNodeBs) and between eNodeBs and core sites including S1, X2, and all other management and timing plane communications between these devices.
    b. Domain Security – Protect the end-to-end network by dividing it into domains; providing protection between domains; providing security policy and procedure for each domain; and ensuring protection of any inter-domain traffic as well as traffic transiting domains. Domains could include the:
        i. Radio Access Network within a State (either FirstNet or opt-out)
        ii. Backhaul Network – eNodeB to regional aggregation points
        iii. Aggregation Network – Aggregation of traffic in a region
        iv. National Transport Networks – Network connection regional and national core sites
        v. Evolved Packet Core
        vi. Business Support Systems
        vii. Operational Support Systems
        viii. Application Ecosystem
        ix. Internet Protocol (IP) Multimedia Sub-System (IMS)
        x. Value-Added Services
        xi. Messaging Services
        xii. PSE Network Connectivity
        xiii. FirstNet Cloud Environments

c. External Interface Protection – Protection of all external interfaces with appropriate security protections such as firewalls, protection from common Internet attack vectors (Denial of Service [DOS], Distributed DOS [DDOS], spoofing, malware, botnets, and port scanning), intrusion prevention and detection, security gateways, security logging and content inspection/filtering. External interfaces may include:
    i. SGi Interface
    ii. Roaming Interfaces such as S8, S6a
    iii. PSTN and Voice over IP (VoIP) Peering for voice and messaging traffic
    iv. PSE Network Interfaces
    v. Network Partner, Network Element Provider, and other third-party remote connection interfaces required for on-call or emergency maintenance and troubleshooting.
    vi. Applications Ecosystem interfaces towards content providers, application developers and service providers offering services via the applications ecosystem.
d. End-to-End Security Management and Logging – The NPSBN should have a security information and event management (SIEM) solution that exposes interfaces to FirstNet. Further details are contained in Section 2.10 Cyber Security Network Management and Configuration Management Policy.
e. Fraud Prevention and Revenue Assurance – The NPSBN should have Fraud Prevention and Revenue Assurance functionality to ensure that resources are being used appropriately and charging and service control transactions are providing a true picture of network usage.
f. Network Address Translation – Network address translation and other associated functions should be implemented for end-user traffic. Where required, static addressing should be available as well.
g. Protection Between Users - Where appropriate, and not at the expense of operability, users should be protected 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 IMS session but attack vectors such as ping-of-death, port scanning and DOS should be prevented between end users.
h. Signaling Storms – Signaling storms should be detected and prevented both inside the network and on external signaling interfaces. This may be accomplished with Diameter Routing Agents and Proxies.
i. Rouge or Stolen Devices- Protection from and against rogue devices and/or stolen devices (i.e., devices deemed to be either a operability or security risk, devices that have been compromised, or devices that have not successfully passed device certification processes). This may include Equipment Identity Register functionality but should also include detection functionality as well. A device or class of devices should be able to be blacklisted/un-blacklisted either manually or automatically. If automatic blacklisting is employed, then blacklisting cannot negatively affect public safety's mission or place first responder lives in jeopardy. This mitigation cannot be done at the expense of leaving a public safety practitioner without emergency communications.
j. Heterogeneous Networks – The NPSBN Cyber Security Solution should enable small cells and heterogeneous networks, potentially offered by a third party, to securely authenticate to and interconnect to the core network.
k. Operational Support System – The Operational Support System should implement FCAPS (fault management, configuration management, accounting management, per-

formance management, and security management), authentication of all users connecting to network elements for maintenance and operations, and logging of all access and configuration actions. Further details are contained in Section 2.10 Cyber Security Network Management and Configuration Management Policy.

l. Domain Name Service (DNS) Security – A secure DNS solution should be deployed as well as 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.
m. Messaging Security – The NPSBN Cyber Security 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.
n. IMS Security – The NPSBN Cyber Security Solution should include an IMS security solution that protects it from an infrastructure, signaling, and user-plane prospective.
o. Business Support Systems Security – The business support systems—including, but not limited to mediation, charging, billing, provisioning, local control, and customer resource management systems—should be protected and include access control and full transactional logging.
p. Mobile Virtual Private Networks (VPNs) – A mobile VPN solution and enablement should ensure public safety entities are able to utilize a secure communications methodology while still able to utilize Quality of Service, Priority, and Preemption. If secure communications are required by public safety for network services such as messaging, FirstNet cloud services, and IP multimedia services, then mobile VPNs should be able to be terminated inside the FirstNet core network.
q. Business Continuity Planning, Disaster Recovery Planning and Crisis Management – The NPSBN Cyber Security Solution should utilize industry best practices for Business Continuity Planning, Disaster Recovery Planning, and Crisis Management.
r. IP Infrastructure Network Elements – All routing and switching network elements should be hardened and configured to only allow traffic that is required to transit through it with access control lists and other methodologies.
s. 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:
    i. Patch maintenance
    ii. A security hardening tool portfolio
    iii. Access control including associated system configuration and policy
    iv. File system hardening and access control
    v. Network security
    vi. Process security
    vii. Host logging
    viii. Time synchronization
t. Cyber Security Governance Model – The cyber security governance model should include 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.

u. Cyber Supply Chain Security – It is critical that the cyber security of the supply chain is verifiable and that no vulnerabilities, exploits, or threat vectors have been introduced to products prior to installation in the NPSBN.
v. Training – It is critical that human factors within cyber security be considered as one of the most important but most difficult areas to assess and protect. Training of users and operators should be one of the keys methods to increase the cyber security of the NPSBN.
w. Insider Threat Mitigation – The NPSBN Cyber Security Solution should include prevention, control, mitigation, and detection of insider threats.
x. Cloud Security – There should be a robust cyber security 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.
y. Virtualization Security – As virtualization becomes more common, even within the Evolved Packet Core through Telco Cloud and Network-Function Virtualization, the cyber security of the virtual environment requires additional focus to ensure there are no cyber risks introduced to the network through virtualization.
z. VoIP Spam – The NPSBN Cyber Security Solution should provide mitigation for VoIP Spam or Spam over Internet Telephony. This should also include mitigation of "robodialing."

3. Devices – User Equipment or Device Security should include, but is not limited to:
    a. Secure Operating System Architecture
        i. Trusted boot loader that initiates the Operating System of the device. To be trusted, boot loaders cannot be allowed to be tampered with by malware. Operating system vendors today now take on the responsibility of building bootloaders into their software instead of employing third party software.
        ii. Every application and even large portions of the operating system should run inside their own isolated sandbox called an AppContainer.[1]
        iii. An AppContainer is a secured isolation boundary that an application and its process can run within. Each AppContainer is defined and implemented using a security policy. The security policy of a specific AppContainer defines the operating system capabilities to which the processes have access within the AppContainer.
        iv. By default, a basic set of permissions is granted to all AppContainers, including access to its own isolated storage location. In addition, access to other capabilities can be declared within the application code itself. Access to additional capabilities and privileges cannot be requested at runtime.
        v. 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.

[1] Android, Windows – Operating System

vi. FirstNet and its selected contractors will work with Device Manufacturers on OS updates related to security issues and Local Control Mobile Device Management (MDM) solutions to enable the PSE to get updates to public safety users.
vii. The device local storage should be encrypted with OS capability.

b. Authentication of the Users and Applications
   i. MDM should enable the PSE Administrator to enforce Device and Application password policies remotely.
   ii. MDM should enable authentication for access to the collection of secured apps on the device.
   iii. Certificate or Token-Based Authentication of certified applications should be available.
   iv. Device-Specific Biometric Authentication (Fingerprint, Retina) should be integrated for supplemental authentication of certified Application access.
c. Embedded Applications
   i. Latency-sensitive Mission Critical applications (such as Mission Critical Push to Talk) should be signed and certified (FirstNet-validated) and should be provided to various original equipment manufacturers as part of pre-installed applications on the Device.
   ii. Internal embedded clients should use non-exposed Access Point Name (APN) for access to FirstNet-certified applications or for PSE network access.
d. MDM and MAM – PSE-Managed Whitelist/Blacklist
   i. The PSE Administrator should be able to wipe or lock a lost or stolen device.
   ii. The PSE Administrator should be able to manage applications on devices through MDM.
e. Digital Signature of the Applications
   i. Digital signatures of signed applications should be verified before publication to the FirstNet app store.
f. 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 user equipment (UE) by the network with content inspection/filtering, messaging security, and the protections provided through other methodologies in this section.
g. Bring Your Own Stuff – Cyber security solutions should address "Bring Your Own (Device, Application, or Wearable)."

4. Application Security – The NPSBN Cyber Security Solution should implement Application Security, which may include but is not limited to:
   a. Applications Ecosystem Security – The solution should provide protection for the FirstNet Applications Ecosystem such as the app store, application development environment, cloud services, Service Delivery Platform (SDP)/Application Programming Interface (API) gateway between NPSBN network services, applications, and the PSE networks. The default public safety applications and data, such as local control and the agency home page portal, need to be secured and protected against external threats, internal threats, data breaches, and DOS attacks.
   b. API Security – FirstNet application developers will develop new NPSBN capabilities and services and expose specific APIs to enable new applications. These APIs, services, and applications will allow for exciting new capabilities such as dynamic control of Quality of Service, priority, preemption, local control, agency home page status, and creation of

public safety analytics. APIs give client-side developers—both legitimate developers and potential system hackers—more finely grained access into an application than a typical Web application. The solution needs to address API threats including, but limited to the following:

i. Parameter attacks that exploit the data sent into an API, including URL, query parameters, HTTP headers, and/or post content.
ii. Identity attacks that exploit authentication, authorization, and session tracking.
iii. Man-in-the-middle attacks that intercept legitimate transactions and exploit unsigned and/or unencrypted data.

c. 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 appropriate information about the user who takes those actions.
d. Application Security in Software Development Lifecycle – The solution should promote secure programming and providing tools to assist developers to ensure they keep security in mind throughout the development process. Currently, there are a number of code analysis and test tools available commercially or through open source as well as many additional resources that developers can leverage. Developers should avoid commonly communicated programming security concerns.
e. Application Security Certification – The solution should ensure FirstNet's application security and certification process includes the analysis of 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 lifecycle is critical. Such tools and assessments should be continually used, even after an application has been certified, because the security landscape continues to change with new risks and vulnerabilities discovered daily. The solution should ensure all Mobile, Web, and Desktop applications operating on the NPBSN 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 FirstNet app store.
f. Application Developer Certification – The application developers registering with FirstNet and publishing the applications should be audited and certified apart from the applications itself.
g. User Logging – The solution should ensure applications properly log and audit the actions by the user and the appropriate information about the user who takes those actions. Proper logging and auditing can provide invaluable information and uncover more than just security concerns.
h. 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 application ecosystem and provide vital security reports and information.
i. Validate the Application Network – It is essential the application network elements and the associated software/hardware be continuously monitored, including the following:

i. All ports and firewall external facing interfaces
ii. FirstNet app store and its portal

iii. FirstNet API Gateway (Northbound interface to PSE, cloud service providers)
iv. NPSBN Gateway to land mobile radio providers
v. FirstNet Application Development Sandbox Environment
vi. FirstNet Application Hosted infrastructure

j. Application Approval and Whitelists – The solution should provide protections to ensure only approved applications are loaded and run on a UE.
k. Application-Device Security – The solution should provide protections to ensure applications cannot bypass OS security on devices.
l. Data Loss Prevention – The solution should provide protections to ensure applications protect data while at rest, in use, and in transit.

5. Strong Authentication/Identity Management – The NPSBN Cyber Security Solution should provide:
   a. ICAM with federated identity from PSE networks.
   b. Identity Assurance – The solution should ensure the following relationships are always authenticated:
      i. User to Device – PSEs may not acquire one device for every user. It therefore becomes critical to know which first responder has the device.
      ii. Device to Network – LTE authentication
      iii. Network to Application – Identity management
      iv. Network to PSE Network – Identity management
      v. User to Application – Identity management
      vi. User to PSE Network – Identity management
6. Utilize Cryptography – LTE is designed with strong cryptographic techniques and mutual authentication between LTE network elements with security mechanisms built into its architecture. However, trusted industry organizations have identified security vulnerabilities that should be assessed by virtue of network deployment. 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.
7. Provide Public Safety Enterprise Network Security – The solution should formulate recommended minimum security standards for state and local agencies. As part of its outreach function, the solution should strive to educate state and local agencies on cyber security topics related to the NPSBN and to review and advise them on strengthening their security architectures and policies if needed prior to connecting to the FirstNet network.

2.3 Cyber Security Lifecycle

1. The cyber security lifecycle will comprise an ongoing process designed to ensure security controls are employed and monitored to ensure continued viability and effectiveness. 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:
   a. Identifying vulnerabilities
   b. Identifying threats
   c. Determining risks arising from threats and vulnerabilities
   d. Prioritizing risks to determine which warrant associated controls to address threats or vulnerabilities
   e. Specifying controls to address or mitigate those threats and vulnerabilities

f. Implementing controls
g. Assessing the effectiveness of controls
h. Monitoring the security of the system

2. Identifying Vulnerabilities
    a. Vulnerabilities can surface in virtually all aspects of the FirstNet enterprise.
    b. It is critical to be aware and capable of identifying those vulnerabilities present in software (OSs, applications, protocols, encryption), hardware, firmware, and related capabilities.
    c. Vulnerabilities will need to be documented appropriately to permit development of suitable controls as well as determine the effectiveness of those controls.
3. Identifying Threats
    a. Threats can take multiple forms and provide attack vectors to all components of the FirstNet enterprise.
    b. The core network, Radio Access Network, user equipment, applications, and even backhaul transport are subject to a range of threats.
    c. The threats will need to be documented appropriately to permit development of suitable controls as well as determine the effectiveness of those controls.
4. Determining Risks Arising from Threats and Vulnerabilities
    a. Once the relevant threats and vulnerabilities have been identified and documented, it will be necessary to determine the risks tied to each.
    b. In some cases, the risk will be sufficiently improbable as to not require any action.
    c. For all others, an impact determination will be accomplished to rank where the risk falls relative to other risks.
5. Prioritizing Risks to Determine Which Warrant Associated Controls to Address Threats or Vulnerabilities
    a. After risks have been assigned respective impact determinations, they will be ranked in order of criticality to determine mitigation.
    b. 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).
    c. Those risks tied to a particular vulnerability or threat will be evaluated based on impact and viability of mitigation.
    d. Upon final ranking and evaluation, appropriate controls will be addressed.
6. Specifying Controls to Address or Mitigate those Threats and Vulnerabilities
    a. Once the threats have been identified, suitable controls will be identified to mitigate them.
    b. In the event, there is no viable control to address a threat, a determination of acceptance of risk and a future proposed fix should be documented and provided in lieu of an available control, including revalidation periodically but no less than quarterly, to determine if the proposed fix is available and if the current acceptance is still sufficient.
7. Implementing Controls
    a. All selected and specified controls will be implemented prior to Initial Operating Capability when possible; those controls developed subsequently or as new ones supersede existing solutions will be implemented as quickly as possible but not before ensuring they do not introduce unanticipated problems elsewhere.
    b. Implementation of controls will adhere to the configuration management and network configuration guidance proposals found later in this document.
8. Assessing the Effectiveness of Controls

   a. After implementation, the effectiveness of the specified controls will be assessed on an ongoing basis to ensure they perform their function as expected.
   b. The results of the ongoing assessment will be documented appropriately and retained for situational awareness.
9. Monitoring the Security of the System
   a. The NPSBN will be monitored from a performance and security perspective and indicators tracked for the security controls and their effectiveness against identified threats.
   b. Monitoring will also be used to develop awareness of new threats and provide the necessary injects to begin the cyber security lifecycle process at the identify threats stage once again.
   c. The overall process is iterative and does not end as new threats and the need for associated security controls continues indefinitely.
10. Key to this ongoing approach will be the necessity of 3GPP Feature Enhancements and Major Release upgrades being made available and implemented on the NPSBN.
11. A plan should exist to address associated support for security upgrades as device capabilities advance generationally.
12. The solution should develop provisions to establish security supportability for aging devices over time and sunset procedures for those devices when they are no longer viable.

2.4 Cyber Security Guidance

There is considerable cyber security guidance available from industry, government, and standards organizations that should be considered when developing the NPSBN Cyber Security Solution. There is no single solution or guidance provided today that can be considered the end-all, be-all for cyber security, and many of them overlap. When considering the complexity of the NPSBN and the fact that its components, users, and usage falls into many different cyber security areas of practice, each of the items listed in this section should be considered and used:

1. The National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, which states, at a minimum, any cyber security solution should:
   a. Describe the current cyber security posture.
   b. Describe the target state for cyber security.
   c. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
   d. Assess progress toward the target state.
   e. Communicate among internal and external stakeholders about cyber security risk.
2. 3GPP LTE Security Standards
   a. Network Access Security – Provide a secure access to the service by the user
   b. Network Domain Security – Protect the network elements and secure the signaling and user data exchange
   c. User Domain Security – Control secure access to mobile stations
   d. Application Domain Security – Establish secure communications over the application layer
   e. User Configuration and Visibility of Security – Provide an opportunity for the user to check if the security features are in operation
3. National Fire Protection Association 1221 Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems, which has a new chapter on data security that is currently out for comment.

4. Federal Bureau of Investigation's (FBI) CJIS Security Policy, which includes all those that support the FBI and Department of Justice [CJISD-ITS-DOC-08140-5.0].
5. NIST Recommendations on Cybersecurity (Special Publications 800 Series)
6. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27003: Network Security
7. ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls
8. ISO/IEC 17799: Information technology – Security techniques – Code of practice for information security management
9. North American Electric Reliability Corporation Critical Infrastructure Protection Regulations
10. U.S. Department of Homeland Security Critical Infrastructure Cyber Community C³ Voluntary Program
11. U.S. Department of Homeland Security National Infrastructure Protection Plan
12. Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity
13. Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience
    a. NPSBN Critical Infrastructure Sector Involvement
        i. Direct Involvement
            1. Emergency Services Sector
            2. Communications Sectors
            3. Government Facilities
        ii. Indirect or Supporting Involvement on Behalf of Public Safety
            1. Healthcare and Public Health Sector
            2. Transportation Systems Sector
            3. Water and Wastewater Systems Sector
            4. Information Technology Sector
            5. Commercial Facilities Sector
14. International Telecommunications Union – Telecommunication Standardization Sector's Recommendations as guidance for the design of the NPSBN Cyber Security Solution
    a. X.800 Coverage of Security and Management
    b. X.805 Security Architecture for Systems Providing End-to-End Communications, which defines the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security.
    c. X.1051 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications organizations based on ISO/IEC 27002. It also provides an implementation baseline of information security management within telecommunications organizations to ensure the confidentiality, integrity, and availability of telecommunications facilities and services.

2.5 Cyber Security Systems Engineering

The International Council on Systems Engineering defines systems engineering as "a profession, a perspective and a process." The NPSBN Cyber Security Solution must take into account the best practices of systems engineering but expand them with the best practices of cyber security engineering. Cyber Security Systems Engineering should:

1. Include a Cyber Security Systems Engineering Plan that enumerates operational policy and procedures to ensure that it is followed at all levels.
2. Include a repeatable process that is executed continuously both during the development and evolution of the NPSBN.
3. Represent a unique perspective into the NPSBN that ensures cyber security engineering is considered in all decisions, designs, and actions.
    a. It should meet the core tenets of cyber security 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.
4. Maintain the simple overarching principles of FirstNet:
    a. Ensuring the network is being used by only the authorized personnel it supports.
    b. Ensuring the network and its users are protected from all others, whether they are external adversaries or insider threats.
    c. Ensuring the cyber security program is robust and capable of detecting if either a. or b. is not true.
5. Ensure the cyber security design of network and components:
    a. Plans, develops, and tests new technologies
    b. Performs technical analysis in support of development and test activity for new systems and emerging technologies.
    c. Facilitates development of future requirements and architecture components to enable transition of new systems and technologies into the operational baseline.
    d. Coordinates future technology efforts with internal and external partners and operational users.
6. Facilitate cyber security assessment:
    a. Utilizes a third-party, independent, outside organization to provide lab and field security assessments.
    b. Performs independent verification of our thinking, planning, and infrastructure.
    c. Brings best practices from other parts of the federal government and industry.
    d. Runs large-scale scheduled cyber security exercises and targeted local cyber security exercises as needed.
7. Utilize resilient design principles, including but not limited to:
    a. Engineering a Resilient Network. This requires balancing single-points-of-failure and economics. In short, it is about understanding and managing risk.
    b. 3GPP Release 8 LTE, which introduces IP as the basic connectivity between network elements.
    c. FirstNet'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:
        i. Self Organizing Networks
        ii. Site Hardening (physical security)
        iii. Layers of Network Coverage
        iv. Industry Best Practices to protect against systemic failures, cyberattacks, and human errors
8. Application Security Policy and Procedure. The solution should establish a process for secure development, verification, and distribution of applications that can be used on the NPSBN.

2.6 Cyber Security Risk Management

1. The program should have a detailed and robust Risk Management Methodology that is executed continuously during the system's development lifecycle and during the life of the program and NPSBN.
2. The Risk Management Methodology should, at a minimum, contain the following steps:
    a. Asset Identification
    b. Risk Impact Analysis
    c. Threat Assessment
    d. Risk Mitigation
    e. Security Control Selection and Deployment
    f. Risk Mitigation Operations and Maintenance
3. The methodology could be based on or enhanced by a number of existing models, such as the NIST Risk Management Framework or the ISO 27000 series. These frameworks are generally meant to enhance existing processes

2.7 Cyber Security Incident Response and Security Operations Center

Incident reporting and response is 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.

1. FirstNet envisions that incident response management will be performed by a Cyber Security Incident Response Team, which should perform the following activities at a minimum:
    a. Coordinate the notification and distribution of an incident.
    b. Mitigate the risk of an incident by minimizing disruptions, and notify the contracting officer if it appears that the mitigation will have an associated cost.
    c. Assemble security staff to conduct a threat analysis and resolve the incident.
    d. Take reasonable steps to mitigate the effects and to minimize any damage resulting from the incident.
    e. Monitor system logs for application to the incident.
    f. Categorize all security incidents per policy and procedure and report them within specific time frames to be identified.
    g. Define and capture metrics that will be used for reporting capability.
    h. Provide a post-mortem for each incident associated with an actual cyberattack in a format agreed upon by the contractor and FirstNet.
    i. 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.
    j. All security incidents are recorded or logged into an electronic format (to be determined). These logs will provide the information for reporting purposes.
    k. All security incidents are reported based on incident severity, as directed in standard operating procedures that will be developed jointly between the contractor and FirstNet.
2. Security Operations Center – The Security Operations Center should provide:
    a. Situational Awareness that includes collecting, maintaining, and sharing information about threats to infrastructure.
    b. 24/7/365 cyber security monitoring of core infrastructure

c. Monitoring and analysis of user, system and network access
d. Assessment of the integrity of the system and data file
e. Establishment of the baseline network activity and utilization to use as a reference
f. Recognition and analysis of activity patterns that are indicative of an incident or intrusion
g. Analysis of logs for abnormal use patterns
h. Information Sharing and Collaboration that integrates and disseminates information throughout the critical infrastructure partnership network. Processing and posting Suspicious Activity Reports.
i. Assessment and Analysis that evaluates infrastructure data for accuracy, importance, and implications.
j. Decision Support that provides recommendations to partners and FirstNet leadership.

All incidents must be immediately reported, whether suspected or confirmed, involving potential risks to the confidentiality, integrity, or availability of FirstNet information or to the function of NPSBN systems operated on behalf of FirstNet. If the FirstNet Security Operations Center determines that a digital forensic analysis is needed for any event or incident, notification of FirstNet leadership is critical.

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

2.8 Cyber Security Continuous Monitoring and Mitigation Methodology

1. Continuous Monitoring (CM) and Forensics – There are a number of active security tools and solutions available on the market today that continuously monitor, log, and provide forensic data about the current state of the network and any changes that have occurred. These tools should be part of the NPSBN Cyber Security Solution.
2. The continuous monitoring approach should include the following components and processes to be effective:
    a. Hardware Asset Management
    b. Software Asset Management
    c. Vulnerability Management
    d. Configuration Settings Management
3. Hardware asset management is 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.
4. Software asset management is 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.
5. Vulnerability Management entails scanning software throughout the network as well as traffic traversing the network for signatures or behavior, which is atypical for the specified network. Items identified in vulnerability scans are then referred for analysis and further investigation.
6. Configuration Settings Management is the component of CM that deals with settings on network components, such as router access control lists or firewall settings. This automated toolset evaluates settings against baseline standards to ensure both consistency of configuration as well as ensuring simple typos do not result in compromising the network.

7. Mitigation of identified issues from CM 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.

2.9 Cyber Security Testing and Certification Plan

1. Testing Lifecycle - Processes should be established to verify security approaches through a lifecycle of selection, procurement, integration, and operations support. This is often a key functionality within an organization's greater cyber security 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.
    a. Assessment is the process whereby a security control is evaluated as to how well it meets stated security objectives.
    b. Testing is the subjection of the security control to inputs to determine what expected and unexpected results occur.
    c. Examination is the review of related documentation for one or more controls to determine stated objectives and capabilities.
    d. Interviewing is the discussion with designers, implementers, and users regarding the expectations and behaviors of the stated controls on the system.
2. Individual System Validation – Consideration should be given to validation of individual systems being performed 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.
3. 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.
4. Independent Applications/Services Testing – All applications that are distributed by the core network or exchange data with the core network will need a formal testing, validation, and authentication process 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. The testing and validation will have to address applications for each of the following situations as appropriate in the lifecycle of the application as well as its origination:
    a. New applications at the national level
    b. User-developed or state-developed applications
    c. Upgrades to currently approved applications
    d. Security patches to currently approved and fielded applications

2.10 Cyber Security Network Management and Configuration Management Policy

1. Network Management
    a. It is critical that all network management for cyber security tools and capabilities be maintained and managed from an out-of-band network that limits access to these devices to a small number of authorized personnel. If this is not practical, then alternative methods, such as VPN, are critical.

2. Configuration Management
    a. In the context of cyber security, Configuration Management is the practice of handling changes to security tools, software, and devices in a repeatable, systemic manner to ensure 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:
        i. Configuration Management Planning and Management
        ii. Configuration Identification
        iii. Configuration Control
        iv. Configuration Status and Accounting
        v. Configuration Verification and Audit
3. Vulnerability Management
    a. Develop a methodology to conduct and maintain routine, consistent vulnerability scanning of FirstNet infrastructure that is passive in nature to ensure no impact to systems, including the efficient, effective remediation of any discovered vulnerabilities.
4. Patch Management
    a. The continuous cycle of applying software updates and patches should address all software provided with the system, including operating systems and third-party applications. Patches should be thoroughly vetted through a verification and validation lab. This will provide FirstNet 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.
    b. Below are industry best practices for a patch management solution:
        i. Centralized role-based administration
        ii. Integration with an Authentication and Authorization Server
        iii. Patch scheduling and administration
        iv. Air-gap patches capability that requires the updating of the Patch Management Server with Mobile Media (e.g., DVD or Thumb Drive) without connectivity to the Internet being required
5. Centralized Security Log Management
    a. Security Information and Event Management – SIEM is 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. The 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.

2.11 Environmental and Physical Security

1. 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 FirstNet wireless network will be disparately deployed across the nation, this can become cost-prohibitive rapidly. Environmental and physical security systems should be capable of monitoring alarms, centrally displaying and reporting 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.
2. High-level areas for consideration in developing physical and environmental security include but are not limited to:
    a. Core Network
        i. Power Failure
        ii. Humidity Detection
        iii. Cabinet Door Alarms
        iv. Uninterruptable Power Supply Power Failure
        v. Access Control to and within a Facility
        vi. Monitoring and Recording of Activity within a Facility to Include Egress/Ingress
        vii. Movement Activity within a Facility After Hours or in Restricted Areas
        viii. Heating, Ventilation, and Air Conditioning (HVAC) Failure or Degradation
        ix. Building Door Alarms
        x. Generator Failure
        xi. Low Generator Fuel
        xii. Low Battery
    b. Radio Access Network
        i. Power Failure
        ii. Cabinet Door Alarms
        iii. UPS Power Failure
        iv. HVAC Failure or degradation
        v. Building Door Alarms
        vi. Generator Failure
        vii. Low Generator Fuel
        viii. Low Battery

2.12 Information Security and Data Sensitivity

1. All data in transit, accessed, or stored across the FirstNet environment will be encrypted and handled as restricted data.
2. The nature of restricted data is that its use, dissemination, and access are limited to specific agencies, individuals, and situations.
3. Where existing data repositories employed by FirstNet users already have established levels of mandated sensitivity and protection, those levels will be used at a minimum.
4. 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 will be destroyed or otherwise disposed per agency policy.
5. Data in the NPSBN will not be releasable to any external parties without compliance with applicable law.

3 Terms of Reference

Aggregation Network	An aggregation network is a regional network that aggregates backhaul traffic toward regional data centers and national transmission networks.
AppContainer	AppContainer refers to the virtual machine construct also referred to as a sandbox, which creates an isolated security boundary around the application to keep its operation isolated from other applications and the operating system.
Application Ecosystem Security	Application ecosystem security refers to the policies, technology, and controls to protect data and applications within the application store, the development environment, and the distribution system from the store to the various user equipment types.
Application Security Certification	Application security certification is the process whereby applications are vetted to ensure compliance with security controls. Applications must be compliant during development and tested in actual operation before being authorized for use on the NPSBN.
Availability	Availability is the third leg of the Confidentiality, Integrity, and Availability triad of information systems security. Availability refers to the availability of information resources. It is critical to ensure the highest levels of availability in all contexts of the FirstNet environment.
Blacklist	A blacklist is an electronic list that indicates devices or applications that are blocked from operating on a network, including blocked websites that may not be accessed.
Bring Your Own Stuff	Bring Your Own Stuff, also called Bring Your Own Technology, refers to the policy of permitting employees to bring personally owned mobile devices (i.e., laptops, tablets, smartphones, and wearables) to their workplace and to use those devices to access privileged company information and applications. The phenomenon is commonly referred to as information technology consumerization.
Centralized Security Log Management	Centralized security log management refers to the policies and technology to store, search, and analyze security logs from host devices, including firewalls, intrusion detection systems, routers, and gateways, across an enterprise to evaluate trends and conduct forensics.
Cloud Security	Cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.
Confidentiality	Confidentiality is the first leg of the Confidentiality, Integrity, and Availability triad of information systems security. It is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people while making sure that the right people can get it. Access must be restricted to those authorized to view the data in question. It is common for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.
Configuration Management	Configuration management is the systems engineering process concerned with ensuring all components in the network environment are maintained in a consistent fashion to ensure standardization and currency. Changes to the components and system are carefully managed and controlled to minimize or prevent disruption as well as facilitate ongoing operations.
Cyber Security Systems Engineering Plan	A cyber security systems engineering plan is a documented process that ensures the sustainability of an organization's cyber security environment. It includes ongoing monitoring, testing, procurement, and validation of existing processes, technology, and policies as well as the requirements for periodic review and updates to ensure hardware, software, processes, and policy continue to be effective in preventing, countering, and surviving cyber threats to the operation of the organization's mission.

Cyber Supply Chain Security	Cyber supply chain security refers to the methods and processes to ensure hardware and software components comprising the NPSBN are acquired from trusted providers and manufacturers to mitigate the risk of malware and other potential vulnerabilities being introduced into the system from within the system itself.
Diameter Routing Agents	A Diameter Routing Agent (DRA) is a functional element in an LTE network that provides real-time routing capabilities to ensure that messages are routed among the correct elements in a network.
Digital Signature	A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.
DNS	The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.
Embedded Application	Embedded application refers to a program that is implemented within a device at a level closer to the physical hardware to ensure optimal performance, reliability, and security. In a smartphone, the phone application would be an example of an embedded application.
Equipment Identity Register	The Equipment Identity Register is a database that contains a record of all the mobile stations that are allowed in a network as well as a database of all equipment that is banned (e.g., because it is lost or stolen).
FirstNet Cloud Environments	FirstNet Cloud Environments or cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources.
Heterogeneous Networks	Mobile experts define a Heterogeneous Network or HetNet as a network with complex interoperation between macrocell, small cell, and in some cases WiFi network elements used together to provide a mosaic of coverage with handoff capability between network elements.
ICAM	Identity, Credential, and Access Management (ICAM) is a process and set of technologies to permit authentication to be accomplished by a consistent set of criteria agreed to by all parties participating in the transaction. This authentication methodology permits the creation and use of roles in addition to the more traditional user ID in order to assign rights, privileges, and access on a contextual basis, as needed.
Integrity	Integrity is the second leg of the Confidentiality, Integrity, and Availability triad of information systems security. It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.
IOC	Initial Operating Capability (IOC) is the state achieved when a capability is available in its minimum usefully deployable form.
Jail Break	Jail break is the act of overriding software limitations on a mobile operating system.
MAM	Mobile application management (MAM) describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and “bring your own” mobile devices.
MDM	Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.

Messaging Services	Messaging services include common wireless services like short messaging service, multimedia messaging services, instant messaging, and email.
Mission Critical Push to Talk	Mission Critical Push To Talk is a work standard for LTE that will permit high-priority voice communications in a manner similar to that employed by land mobile radios today.
Patch Management	Patch management is the systems engineering process to control what patches should be applied to which systems at a specified time in the enterprise. It includes the testing processes and methodologies to preclude inadvertently breaking systems as a result of applying patches.
PSTN	Public Switched Telephone System (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication.
Risk	Risk refers to the likelihood of a threat or vulnerability to occur or be exploited and the impact such an event would entail to the organization. Risks can be accepted, mitigated, or transferred.
Rogue Application	A rogue application is a program or other code that does not conform to normal security and application constraints on a device or system; it typically takes the form of a virus or other malware.
Rooted	Rooted refers to the act of overriding software limitations on a mobile operating system.
S1	S1 is the reference point between the eNodeb and the Evolved Packet Core elements: Mobility Management Entity and Serving Gateway.
S6a	S6a enables the transfer of subscription and authentication data for authenticating/authorizing user access between the Mobility Management Entity and the Home Subscriber Server.
S8	S8 is a reference point between two roaming networks providing user and control plane messaging between the home and visited networks
SGi	SGi is the reference point between the Packet Data Network Gateway and the packet data network. Typically the packet data network may connect to services like messaging, private networks or the Internet.
SIEM	Security information and event management (SIEM) is a term for software products and services combining security information management and security event management. SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.
Signaling Storm	A signaling storm is a scenario where the signaling traffic within a network has increased, due to some incident or occurrence, beyond the network's ability to handle the signaling traffic.
SOC	A Security Operations Center or SOC refers to the people, processes, and technologies involved in providing situational awareness through the detection, containment, and remediation of information technology threats. A SOC manages incidents for the enterprise, ensuring they are properly identified, analyzed, communicated, actioned/defended, investigated, and reported. The SOC also monitors applications to identify a possible cyberattack or intrusion (event) and determine if it is a real, malicious threat (incident) and if it could have a business impact.
Threat	A threat is an event that has an impact on the organization but generally cannot be controlled (e.g., terrorist attack, earthquake). The risk or risks associated with threats can be mitigated or otherwise addressed.
User logging	User logging refers to the process and tools to track activity on the network to ensure that users are able to access those resources they require and that unauthorized users are not able to access data or other resources.

Value-Added Services	Value-Added Services refers to services beyond telephony like Short Messaging Service or Multi-Media Messaging Service.
Virtualization Security	Virtualization security refers to the policies, technology, and controls to protect data and applications by running them in a software-defined portion of memory as a self-contained machine that can be logically and functionally isolated from the primary device hardware and operating system to prevent attacks against or from the items running in the virtual machine.
VoIP	Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet.
Vulnerability	A vulnerability is a weakness that allows an attacker to reduce a system's security and potentially compromise data and access.
Whitelist	A whitelist is an electronic list maintained to indicate either devices or applications that are permitted to operate on a network, including allowed websites that may be accessed.
X2	X2 is a reference point between eNodeBs for signaling and handover of user traffic between eNobeBs.