Executive Committee Meeting

December 4, 2015

1:30PM

This booklet was prepared by FloridaNet using funds under award 12-10-S13012 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC, or FirstNet.

Agenda

I. Chair Remarks—Terry L. Rhodes

II. Roll Call

1. Executive Committee Members — EXH. A

III. Public Comment

IV. Executive Committee Members - Call for Vote

1. Department of Management Services—Bill Rogers Bio — EXH. B
2. Executive Committee Vacancies — EXH. C

V. FirstNet Updates — EXH. D

1. Cybersecurity Notice — EXH. E
   - i. Appendix C-10 — EXH. F
2. Final Interpretation—1st Notice — EXH. G
   - i. Notice — EXH. H
3. Final Interpretation—2nd Notice — EXH. I
   - i. Notice — EXH. J
4. Consultation Questions & Answers — EXH. K

VI. FloridaNet Updates

1. Overview — EXH. L
2. Technical Committee Activities
   - i. Draft RFP Response — EXH. M
     - a. Florida's Response *(abbr.)* — EXH. N
   - ii. Cybersecurity Notice Response Overview — EXH. O
     - a. Florida's Submittal — EXH. P
   - iii. Contract Vehicle Survey White Paper — EXH. Q
     - a. Paper *(abbr.)* — EXH. R
   - iv. Data Collection Overview — EXH. S
   - v. FirstNet Data Review — EXH. T
   - vi. FirstNet Maps — EXH. U
3. Budget Overview — EXH. V
4. Project Plans (FloridaNet vs. FirstNet) — EXH. W

VII. Upcoming Events — EXH. X

VIII. Previous Meeting Minutes — EXH. Y

Executive Committee

Chair: Terry L. Rhodes, Department of Highway Safety and Motor Vehicles

Governor's Office: Jason Allison, Chief Information Officer

Homeland Security Advisor: Donna Uzzell, Florida Department of Law Enforcement

Florida Police Chiefs Association: Daniel Alexander, Boca Raton Police Department

Tribal Representative: Bobby Brown, Seminole Tribe of Florida

Tribal Representative: Ray Weeks, Miccosukee Tribe

Florida Sheriffs Association: Steve Casey, Executive Director

Department of Management Services: Vacant

Department of Emergency Management: Phil Royce, SWIC

Florida Department of Health: Mike McHargue

. ***Ex Officio:*** *Dr. Joe Nelson, Florida EMS Advisor*

Ex Officio: *John Wilgis, Florida Hospital Association*

Ex Officio: *April Henkel, Florida Health Care Association*

Ex Officio: *Dr. Peter Pappas, Holmes Regional Medical Center, SparrowNet*

Technical Committee Chair: Greg Holcomb, Lake County Public Safety

Finance Committee Chair: Vacant

Florida Department of Economic Opportunity: Sherri Martin, Rural Economies

Private Sector: Mike Sole, Florida Power & Light

Private Sector: Vacant

Florida Fire Chiefs Association: *Kevin Herndon, Deputy Chief (Retired)*

State-wide EMS Representative: Greg Rubin, Miami-Dade Fire Rescue

Florida Army National Guard: Major Ralph Sullenberger

DMS Representative

Department of Management Services

Bill Rogers

Director
Florida Department of Management Services
Division of Telecommunications

Bill Rogers serves as the Director of the DMS Division of Telecommunications. A globally recognized business and technology leader, Rogers has more than 25 years of experience building, growing and managing organizations through information technology and telecommunications.

In 2011, Governor John Lynch appointed Rogers as New Hampshire's Chief Information Officer. He led the Department of Information Technology, managing and coordinating the state's technology resources while developing and implementing strategies that enhanced services and created efficiencies through innovation, information and technology.

Prior to his public service, Rogers held leadership roles within global companies, including FIRST, Goss International, AlixPartners, Johnson Controls, Deloitte Consulting and Honeywell. He served in senior leadership positions in sales and marketing, operations, information technology, engineering, finance, strategic planning, and customer service.

Rogers has a history of commitment to civic and charitable organizations. He served the American Red Cross as Chairman of the Board for the Great Bay New Hampshire Chapter. He has been a keynote speaker and panelist at conferences including NASCIO, The CIO Executive Summit, and the MIT Sloan CIO Symposium. Rogers earned a Master of Science in business administration from Central Michigan University, and a Bachelor of Science in information systems management from the University of Maryland. He is also trained as a Six Sigma Process Owner and Champion. He lives in Tallahassee with his wife, Sue, and their two Labrador Retrievers.

Executive Committee Vacancies

Private Partner

- Colin Denney from Verizon has left the committee

Florida Fire Chiefs Association

- Kevin Herndon has retired

Finance Chair

- No one has been assigned

FirstNet Updates

Since June 26th Executive Committee Meeting

- Received Draft RFP Responses—July 27, 2015
- Organizational changes
    - TJ Kennedy—President
    - Mike Poth—CEO
- FirstNet's 2nd Industry Day—August 27, 2015
- Complete with first round of consultations
- 2nd SPOC meeting—October 7-9, 2015
- Released Cybersecurity Notice—October 2015
- Released Final Interpretations of 1st & 2nd RFCs
- Will release Final RFP by the end of the year

Cybersecurity Notice

- **Released notice 10/5/15**
- **FirstNet recognizes that both usability and security will be equally important to the success of the network and fortunately security can be implemented at the outset**
- **The notice outlines, at a high level, the key considerations and concerns with respect to how our cyber security should be designed, established, and sustained as the foundation of the network**
- **Will assist industry and public safety stakeholders in planning for robust and usable cyber security framework**
- **Opportunity to innovate and be creative in addressing concerns**
- **NPSBN Cyber Security Concepts:**
    - Key Concepts
    - Architecture
    - Lifecycle
    - Guidance
    - Systems Engineering
    - Risk Management
    - Incident Response and Security Operations Center
    - Continuous Monitoring and Mitigation Methodology
    - Testing and Certification Plan
    - Network Management and Configuration Management Policy
    - Environmental and Physical Security
    - Information Security and Data Sensitivity

Appendix C-10
NPSBN
Cyber Security

Nationwide Public Safety Broadband Network (NPSBN)

10/5/2015

Table of Contents

1 **Introduction** **2**
2 **NPSBN Cyber Security Concepts** **4**
2.1 Cyber Security Key Concepts 4
2.2 Cyber Security Architecture 5
2.3 Cyber Security Lifecycle 11
2.4 Cyber Security Guidance 13
2.5 Cyber Security Systems Engineering 14
2.6 Cyber Security Risk Management 16
2.7 Cyber Security Incident Response and Security Operations Center 16
2.8 Cyber Security Continuous Monitoring and Mitigation Methodology 17
2.9 Cyber Security Testing and Certification Plan 18
2.10 Cyber Security Network Management and Configuration Management Policy 18
2.11 Environmental and Physical Security 20
2.12 Information Security and Data Sensitivity 20
3 **Terms of Reference** **21**

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.

Final Interpretation—1st Notice

FirstNet provided their final interpretation on the first notice which focused on the following items:

- **Core network**
  - *Defined as the standard Evolved Packet Core elements under 3GPP standards, device services, location services, billing functions, and all other network elements and functions other than the RAN*
  - *The national and regional data centers, and other elements and functions that may be distributed geographically...and provide connectivity between the RAN and the public Internet/public switched network*
- **Radio access network**
  - *All cell site equipment, antennas, and backhaul equipment….that are required to enable wireless communications with devices using the public safety broadband spectrum…*
  - *Consisting of the standard E-UTRAN elements and including, but not limited to, backhaul to FirstNet designated consolidation points*
  - *State choosing to conduct its own deployment of RAN must use the FirstNet core*

  Florida initially agreed with these definitions. Florida was concerned about the network architecture and the possibilities of others building 'cores', and how those would connect. According to the Act, FirstNet is the only entity responsible for constructing a core network. States choosing to build their own RAN, will have to pay fees to access the Core.
- **Legal scope of all potential users of the NPSBN, including**
  - public safety entities,
  - secondary users,
    - *Any user that seeks access to or use of the NPSBN for non-public safety services*

  Florida agreed that secondary users were essential for the financial stability, but were concerned with how much excess capacity would be granted the secondary users. There should be assurance that Public Safety would get priority and preemption. FirstNet believes that the 20MHz along with priority/preemption capabilities will prevent any negative impact on public safety's use.
  - and other unspecified users
- **Consumer**
  - *Does not include any PSE defined in the Act, States seeking access, entities seeking access*
- **FirstNet's potential service offerings**
- **Opt-out States' potential service offerings**
- **RFP process**
  - *Conclusion: complying with FAR satisfies the open, transparent, and competitive requirements*
- **Minimum technical requirements for the NPSBN**

Final Interpretation—1st Notice

    - *FirstNet may make changes to minimum technical requirements developed by the Interoperability Board*

- **Rural**
    - *Any area that is NOT a city, town, or incorporated area that has a population of greater than 20,000 inhabitants*
    - *Any area that is NOT any urbanized area contiguous and adjacent to a city or town that has a population of greater than 50,000 inhabitants*
- **Substantial rural milestones**
- **Leveraging Existing Infrastructure**
    - *Proposals are required to leverage partnerships with commercial mobile providers where economically desirable*
    - *Factors other than cost that might be utilized in assessing whether existing infrastructure is "economically desirable": infrastructure type/characteristics, security, suitability/viability, readiness for reuse, scope of use, availability/accessibility, any use restrictions, relationships with infrastructure owners/managers, available alternatives in the area*
- **Network user fees**
    - *FirstNet may charge a fee to any user that seeks access to or use of the NPSBN*
    - *States assuming RAN responsibility can be assessed fees that are in addition to those under the Act*

    Florida proposed that for opt-out scenarios, fees should be limited to core and spectrum use fees and should not include a FirstNet user fee either in State or while roaming to other states.

- **Lease fees related to network capacity**
    - *CLA does not require a secondary user, multiple CLA lessees could coexist, the lessee must do more than a nominal amount of constructing, managing, or operating the network, entity in agreement does not have to perform all areas as long as they do what they agreed upon under their agreement.*
    - *'Network Capacity' - combination of spectrum and network elements and including the core network as well as the RAN of either FirstNet alone or that of a secondary user under a CLA. The core and RAN are to be used for both FirstNet public safety and the secondary's users commercial customers. The Act does not provide any cap or limitation on how much can be used by a secondary user.*
    - *'Secondary basis' - the network capacity will be available to the secondary user unless it is needed for public safety entities.*
    - *'Spectrum allocated to such entity' - allowing all or a portion of the spectrum licensed to FirstNet by the FCC under call sign "WQQE234" to be allocated for use on a secondary basis under a CLA. FirstNet has the duty to ensure the establishment of the network and has to ensure the efficient use of the funding resources available to fulfill the duty.*

Final Interpretation—1st Notice

Florida requested that each State should determine how much capacity/spectrum should be available within its borders for CLAs since it does not require any minimum amount of spectrum to be allocated.

- *FirstNet is the sole entity responsible for determining how to allocate the spectrum under the CLA.*

- *'Dark fiber' - will allow the CLA lessee to transport traffic on otherwise previously dark fiber facilities*

- **Network equipment and infrastructure fees**
  - *Limit the imposition of a fee for the use of static or isolated equipment or infrastructure*
  - *'Constructed or otherwise owned by FirstNet' - FirstNet either paid for equipment or contracts the access to the equipment*
- **Ex Parte communications**

to secondary users on a statewide, regional, or national basis—whichever arrangement is most profitable.

Response: FirstNet agrees that it should evaluate various funding and deployment options in order to help speed deployment and ensure the establishment of a self-sustaining broadband network dedicated to public safety throughout the nation.

Comment #65: One commenter suggested that, although revenue generated from a covered leasing agreement is an important financial contribution to the construction and maintenance of the nationwide network, FirstNet should not allow the promise of secondary leasing agreements to single-handedly drive its strategic decisions.

Response: FirstNet acknowledges the comment and intends to analyze and determine the most efficient and effective way to utilize its various funding streams to ensure the deployment and operation of a nationwide broadband network for public safety.

Comment #66: One commenter suggested that State law, not FirstNet, should determine the ability of an opt-out State to profit from public-private partnerships or covered leasing agreements.

Response: The Act authorizes States to enter into covered leasing agreements with secondary users through public-private arrangements and establishes the parameters of those arrangements.[85] Indeed, the Act explicitly limits the use of any revenue gained by a State through a covered leasing agreement to constructing, maintaining, operating, or improving the RAN of that State.[86] Similarly, FirstNet has also concluded that section 1428(d), authorizing a State to enter into public-private partnerships, was intended by Congress to be read consistently, to the extent such an arrangement is considered something different from a covered leasing agreement, so as to ensure ongoing reinvestment of all revenues into the network. This is consistent with the overall purpose and intent of the Act to ensure the deployment and operation of the NPSBN.

Dated: October 15, 2015.

Jason Karp,

Chief Counsel (Acting), First Responder Network Authority.

[FR Doc. 2015–26622 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–TL–P

[85] *See* 47 U.S.C. 1442(g)(2).

[86] *See id.*

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket Number: 140821696–5908–04]

RIN 0660–XC012

First Responder Network Authority; Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012

AGENCY: First Responder Network Authority, National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice; final interpretations.

SUMMARY: The First Responder Network Authority (''FirstNet'') publishes this *Notice* to issue final interpretations of its enabling legislation that will inform, among other things, forthcoming requests for proposals, interpretive rules, and network policies. The purpose of this Notice is to provide stakeholders FirstNet's interpretations on many of the key preliminary interpretations presented in the proposed interpretations published on September 24, 2014.

DATES: Effective October 20, 2015.

FOR FURTHER INFORMATION CONTACT: Eli Veenendaal, First Responder Network Authority, National Telecommunications and Information Administration, U.S. Department of Commerce, 12201 Sunrise Valley Drive, M/S 243, Reston, VA 20192; 703–648–4167; or *elijah.veenendaal@firstnet.gov*.

SUPPLEMENTARY INFORMATION:

I. Introduction and Background

The Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112–96, Title VI, 126 Stat. 256 (codified at 47 U.S.C. 1401 *et seq.*)) (the ''Act'') established the First Responder Network Authority (''FirstNet'') as an independent authority within the National Telecommunications and Information Administration (''NTIA''). The Act establishes FirstNet's duty and responsibility to take all actions necessary to ensure the building, deployment, and operation of a nationwide public safety broadband network (''NPSBN'').[1]

One of FirstNet's initial steps in carrying out this responsibility under the Act is the issuance of open, transparent, and competitive requests for proposals (''RFPs'') for the purposes of building, operating, and maintaining the network. We have sought—and will continue to seek—public comments on many technical and economic aspects of these RFPs through traditional procurement processes, including requests for information (''RFIs'') and potential draft RFPs and Special Notices, prior to issuance of RFPs.[2]

As a newly created entity, however, we are also confronted with many complex legal issues of first impression under the Act that will have a material impact on the RFPs, responsive proposals, and our operations going forward. Generally, the Administrative Procedure Act (''APA'')[3] provides the basic framework of administrative law governing agency action, including the procedural steps that must precede the effective promulgation, amendment, or repeal of a rule by a federal agency.[4] However, 47 U.S.C. 1426(d)(2) provides that any action taken or decision made by FirstNet is exempt from the requirements of the APA.

Nevertheless, although exempted from these procedural requirements, on September 24, 2014, FirstNet published a public notice entitled ''Proposed Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012'' (hereinafter ''the *First Notice*''),[5] seeking public comments on preliminary interpretations, as well as technical and economic issues, on certain foundational legal issues to help guide our efforts in achieving our mission.

The purpose of this *Notice* is to provide stakeholders notice of the final legal interpretations on many of the key preliminary interpretations presented in the *First Notice*. Additional background and rationale for this action and explanations of FirstNet's interpretations were included in the *First Notice* and are not repeated herein. The section immediately below labeled ''Final Interpretations'' summarizes FirstNet's final interpretations with respect to the *First Notice*. Thereafter, the section labeled ''Response to Comments'' summarizes the comments

[1] 47 U.S.C. 1426(b).

[2] The pronouns ''we'' or ''our'' throughout this *Notice* refer to ''FirstNet'' alone and not FirstNet, NTIA, and the U.S. Department of Commerce as a collective group.

[3] *See* 5 U.S.C. 551–59, 701–06, 1305, 3105, 3344, 5372, 7521.

[4] *See* 5 U.S.C. 551–559. The APA defines a ''rule'' as ''the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency and includes the approval or prescription for the future of rates, wages, corporate or financial structures or reorganizations thereof, prices, facilities, appliances, services or allowances therefor or of valuations, costs, or accounting, or practices bearing on any of the foregoing.'' 5 U.S.C. 551(4).

[5] 79 FR 57058 (September 24, 2014).

received on the preliminary interpretations contained in the *First Notice* and provides FirstNet's responses to such comments, including further explanations and any changes to FirstNet's interpretations.

II. Final Interpretations

A. FirstNet Network

Final Definitions of Core Network and Radio Access Network

1. FirstNet defines the core network in accordance with 47 U.S.C. 1422(b) of the Act, relevant sections of the Interoperability Board Report, and commercial standards, as including, without limitation, the standard Evolved Packet Core elements under the 3rd Generation Partnership Project (''3GPP'') standards (including the Serving and Packet Data Network Gateways, Mobility Management Entity, Home Subscriber Server, and the Policy and Charging Rules Function), device services, location services, billing functions, and all other network elements and functions other than the radio access network.

2. FirstNet defines the radio access network in accordance with 47 U.S.C. 1422(b) of the Act, commercial standards, and the relevant sections of the Interoperability Board Report, as consisting of the standard E–UTRAN elements (*e.g.,* the eNodeB) and including, but not limited to, backhaul to FirstNet designated consolidation points.

3. FirstNet concludes that a State choosing to conduct its own deployment of a radio access network under 47 U.S.C. 1442(e) must use the FirstNet core network to provide public safety services within the State.

B. Users

Network Users

4. FirstNet defines a ''secondary user'' as any user that seeks access to or use of the NPSBN for non-public safety services.

Prohibition on Providing Commercial Services to Consumers

5. The definition of ''consumers'' as used in 47 U.S.C. 1432 does not include:

a. any public safety entity as defined in the Act;

b. States when seeking access to or use of the core network, equipment, or infrastructure; or

c. entities when seeking access to or use of equipment or infrastructure.

6. The language of the Act under 47 U.S.C. 1432 prohibiting FirstNet from directly serving ''consumers'' does not limit potential types of public safety entities that may use or access the NPSBN for commercial telecommunications or information services.

7. The Act under 47 U.S.C. 1432 does not prohibit or act as a limit on secondary users with which FirstNet may enter into a covered leasing agreement.

8. The Act under 47 U.S.C. 1432 does not limit the pool of secondary users that may gain access to or use of the network on a secondary basis.

C. Requests for Proposals

Requests for Proposals Process

9. FirstNet, to the extent it utilizes the FAR, concludes that complying with the FAR satisfies the open, transparent, and competitive requirements of 47 U.S.C. 1426(b)(1)(B).

Minimum Technical Requirements

10. FirstNet concludes that it may make non-material changes or additions/subtractions to the minimal technical requirements developed by the Interoperability Board, including as necessary to accommodate advancements in technology as required by the Act.

Final Definition of ''Rural''

11. FirstNet defines ''rural,'' for the purposes of the Act, as having the same meaning as ''rural area'' in Section 601(b)(3) of the Rural Electrification Act of 1936, as amended (''Rural Electrification Act''). Section 601(b)(3) of the Rural Electrification Act provides that ''[t]he term 'rural area' means any area other than—(i) an area described in clause (i) or (ii) of Section 1991(a)(13)(A) of this title [section 343(a)(13)(A) of the Consolidated Farm and Rural Development Act]; and (ii) a city, town, or incorporated area that has a population of greater than 20,000 inhabitants.'' In turn, the relevant portion of Section 343(a)(13)(A) of the Consolidated Farm and Rural Development Act explains that the ''terms 'rural' and 'rural area' mean any area other than—(i) a city or town that has a population of greater than 50,000 inhabitants; and (ii) any urbanized area contiguous and adjacent to a city or town described in clause (i).'' Thus, as defined herein, the term ''rural'' means any area that is *not:*

- A city, town, or incorporated area that has a population of greater than 20,000 inhabitants
- any urbanized area contiguous and adjacent to a city or town that has a population of greater than 50,000 inhabitants

12. FirstNet concludes that a lower boundary (*e.g.,* ''wilderness,'' ''frontier'') is not necessary to satisfy its rural coverage requirements under the Act, and thus FirstNet does *not* intend to establish any such boundary.

Existing Infrastructure

13. FirstNet interprets that 47 U.S.C. 1426(b)(1)(B) is intended to require FirstNet to encourage, through its requests, that responsive *proposals* leverage existing infrastructure in accordance with the provision.

14. FirstNet interprets 47 U.S.C. 1426(b)(3) as requiring FirstNet to include in its RFPs that such proposals leverage partnerships with commercial mobile providers where economically desirable.

15. FirstNet concludes that factors other than, or in addition to, cost may be utilized in assessing whether existing infrastructure is ''economically desirable,'' including:

a. infrastructure type/characteristics

b. security (physical, network, cyber, etc.)

c. suitability/viability (ability to readily use, upgrade, and maintain)

d. readiness for reuse (*e.g.,* already in use for wireless communications)

e. scope of use (*e.g.,* range of coverage)

f. availability/accessibility (time/obstacles to acquiring access/use)

g. any use restrictions (*e.g.,* prohibitions/limitations on commercial use)

h. relationships with infrastructure owners/managers (*e.g.,* ease/difficulty in working with owners/managers)

i. available alternatives in the area

D. Fees

General

16. FirstNet interprets each of the fees authorized by the Act, including user or subscription fees authorized by 47 U.S.C. 1428(a)(1), covered leasing agreement fees authorized by 47 U.S.C. 1428(a)(2), lease fees related to network equipment and infrastructure authorized by 47 U.S.C. 1428(a)(3), and the fee for State use of elements of the core network authorized by 47 U.S.C. 1442(f), as distinct and separate from each other and may be assessed individually or cumulatively, as applicable.

Network User Fees

17. FirstNet concludes it may charge a user or subscription fee under 47 U.S.C. 1428(a)(1) to any user that seeks access to or use of the NPSBN.

State Core Network User Fees

18. FirstNet concludes that the fees assessed on States assuming RAN responsibilities for use of the core network authorized by 47 U.S.C. 1442(f)

are distinct from and can be assessed in addition to any other fees authorized under the Act.

Lease Fees Related to Network Capacity and Covered Leasing Agreements

19. FirstNet concludes that a covered leasing agreement under 47 U.S.C. 1428(a)(2) does not require a secondary user to ''construct, manage, and operate'' the entire FirstNet network, either from a coverage perspective or exclusively within a specific location.

20. FirstNet concludes that multiple covered leasing agreement lessees could coexist and be permitted access to excess network capacity in a particular geographic area.

21. FirstNet interprets that a covered leasing agreement lessee satisfies the definition under 47 U.S.C. 1428(a)(2) so long as the lessee does more than a nominal amount of constructing, managing, or operating the network.

22. FirstNet concludes that an entity entering into a covered leasing agreement under 47 U.S.C. 1428(a)(2) is not required to perform all three functions of constructing, managing, and operating a portion of the network, so long as one of the three is performed as part of the covered leasing agreement.

23. FirstNet interprets the reference to ''network capacity'' in the definition of covered leasing agreement under 47 U.S.C. 1428(a)(2)(B)(i) as a generic statement referring to the combination of spectrum and network elements, as defined by the Act, and including the core network as well as the radio access network of either FirstNet alone or that of the secondary user under a covered leasing agreement, whereby the core and radio access network are used for serving both FirstNet public safety entities and the secondary user's commercial customers.

24. FirstNet interprets the term ''secondary basis'' under 47 U.S.C. 1428(a)(2)(B)(i) to mean that network capacity will be available to the secondary user unless it is needed for public safety entities as defined in the Act.

25. FirstNet interprets the phrase ''spectrum allocated to such entity'' found in 47 U.S. § 1428(a)(2)(B)(ii) as allowing all or a portion of the spectrum licensed to FirstNet by the Federal Communications Commission (''FCC'') under call sign ''WQQE234'' to be allocated for use on a secondary basis under a covered leasing agreement.

26. FirstNet concludes that the reference to ''dark fiber'' in 47 U.S.C. 1428(a)(2)(B)(ii) cannot literally be interpreted as such, and the reference should be interpreted to allow the covered leasing agreement lessee to transport such traffic on otherwise previously dark fiber facilities.

Network Equipment and Infrastructure Fee

27. FirstNet interprets 47 U.S.C. 1428(a)(3) as being limited to the imposition of a fee for the use of static or isolated equipment or infrastructure, such as antennas or towers, rather than for use of FirstNet spectrum or access to network capacity.

28. FirstNet interprets the phrase ''constructed or otherwise owned by [FirstNet]'' under 47 U.S.C. 1428(a)(3) as meaning that FirstNet ordered or required the construction of such equipment or infrastructure, paid for such construction, simply owns such equipment, or does not own but, through a contract has rights to sublease access to, or use of, such equipment or infrastructure.

III. Response to Comments

FirstNet received 63 written comments to the *First Notice* from various stakeholders, including States, tribes, public safety organizations, commercial carriers, equipment vendors, utilities, and various associations. Comments on the *First Notice* included a large number of identical or similar written comments as well as oral statements made during meetings with FirstNet. FirstNet has carefully considered each of the comments submitted. It has grouped and summarized the comments according to common themes and has responded accordingly. All written comments can be found at *www.regulations.gov*.

A. FirstNet Network

1. Final Definitions of Core Network and Radio Access Network

The Act requires FirstNet to ''ensure the establishment of a nationwide, interoperable public safety broadband network'' that is ''based on a single national network architecture.'' [6] This national network architecture must be capable of evolving with technological advancements and initially consists of two primary network components: A *core network* and a *radio access network*.[7] The Act defines the ''core network'' as consisting of ''the national and regional data centers, and other elements and functions that may be distributed geographically . . . and provid[ing] connectivity between (i) the radio access network; and (ii) the public Internet or public switched network, or both . . . .'' [8] Comparably, the Act defines the ''radio access network'' as consisting of ''all cell site equipment, antennas, and backhaul equipment . . . that are required to enable wireless communications with devices using the public safety broadband spectrum . . . .'' [9]

In the *First Notice,* FirstNet made preliminary interpretations further describing the scope of the definitions of the core network and RAN. Although the vast majority of commenters agreed with the interpretations, some expressed concerns that many of the key elements of the network were either not referenced or did not meet the criteria described in the proposed definitions. In response to these comments, FirstNet has slightly modified its preliminary interpretation of the ''core network'' to include the Mobility Management Entity within the Evolved Packet Core elements under the 3GPP standards and its preliminary interpretation of ''radio access network'' to include backhaul to FirstNet designated consolidation points. Accordingly, FirstNet makes the following final interpretations related to the definitions of the core network and radio access network under the Act.

(1) FirstNet defines the core network in accordance with 47 U.S.C. 1422(b) of the Act, relevant sections of the Interoperability Board Report, and commercial standards, as including, without limitation, the standard Evolved Packet Core elements under the 3GPP standards (including the Serving and Packet Data Network Gateways, Mobility Management Entity, Home Subscriber Server, and the Policy and Charging Rules Function), device services, location services, billing functions, and all other network elements and functions other than the radio access network.

(2) FirstNet defines the radio access network in accordance with 47 U.S.C. 1422(b) of the Act, commercial standards, and the relevant sections of the Interoperability Board Report, as consisting of the standard E–UTRAN elements (*e.g.,* the eNodeB) and including, but not limited to, backhaul to FirstNet designated consolidation points.

Analysis of and Responses to Comments on Definition of Core Network and Radio Access Network

Summary: The majority of commenters agreed with FirstNet's proposed definitions of ''core network'' and ''radio access network'' and supported FirstNet considering

[6] 47 U.S.C. 1422.

[7] 47 U.S.C. 1422(b).

[8] 47 U.S.C. 1422(b)(1).

[9] 47 U.S.C. 1422(b)(2)(B).

commercial standards, as well as the relevant sections of the Interoperability Board Report and relevant 3GPP standards, to provide further clarity around the elements and functions of the core network and radio access network.

Comment #1: A few commenters suggested that FirstNet simply use the definitions of the terms ''core network'' and ''radio access network'' that are provided in the statute. For example, one commenter recommended FirstNet use its wide discretion to consider other interpretations as it carries out its responsibilities to implement these network components and not use the Interoperability Board Report to help derive any legal interpretations of the Act.

Response: FirstNet agrees that the Act provides it with broad discretion to carry out its mission. In view of that discretion, FirstNet has determined that it is important to provide additional clarity around certain delineation points between the core network and RAN as defined in the Act. These delineation points become especially important in light of the provisions of 47 U.S.C. 1442(e) that allow a State the opportunity, under certain conditions, to conduct the deployment of a RAN within that State and require that State to pay a fee for use of elements of the core network. In response to the specific example, the Act commissioned the development of the Interoperability Board Report to provide recommended technical requirements to ensure a nationwide level of interoperability for the NPSBN.[10] Under the Act, these recommendations are intended to be used by FirstNet to help develop and maintain the NPSBN.[11] Moreover, a State choosing to assume RAN responsibilities must demonstrate compliance with the minimum technical interoperability requirements of the Interoperability Board Report in order to receive approval of an alternative RAN plan.[12] Based on these provisions, FirstNet believes that it is important to give credence to the relevant sections of the Interoperability Board Report that relate to the definitions of the core network and RAN.

Comment #2: One commenter suggested the proposed definition of the core network is too expansive and recommended that FirstNet remove the language ''device services'' and ''all other network elements and functions other than the radio access network'' from its proposed definition of the core network.

Response: FirstNet disagrees that the proposed definition of core network is too expansive and believes its proposed interpretation, including the language ''device services'' and ''all other network elements and functions other than the radio access network,'' is consistent with both the intent of the Act as well as commercially accepted standards for elements generally comprising a core network. Additionally, FirstNet's inclusion of these terms and phrases in its interpretation assist in providing clarity relating to the definitions of core network and RAN that are critical to establishing the NPSBN and providing the scope of responsibility a State will assume should it decide to conduct its own RAN deployment. In delivering a plan to a Governor for a determination of whether to assume responsibilities for RAN construction, FirstNet must delineate between what elements of the network in the proposed plan comprise the core network versus the elements that comprise the RAN. Accordingly, an understanding of the elements that make up the core network and RAN are critical for a Governor to make an effective determination about whether the State should have FirstNet conduct the RAN deployment or seek to conduct its own RAN deployment.

Comment #3: One commenter expressed concern that the proposed definitions conflate issues of policy and technology and suggested FirstNet avoid rigid definitions of ''core network'' or ''radio access network'' and align their technical and business development efforts with standards that evolve with the long term evolution (''LTE'') broadband network.

Response: FirstNet acknowledges the comment, but believes its proposed definitions of core network and RAN provide additional certainty that is necessary in order to build, operate, and maintain the NPSBN, while, at the same time, preserving, as contemplated by the Act, the necessary flexibility to take into account new and evolving technological advancements. For example, FirstNet's interpretations of both the core network and RAN are inclusive of the language of 47 U.S.C. 1422(b) that specifically states the national architecture must ''*evolve[] with technological advancements* and *initially* consists of'' the stated core network and RAN components.[13] The use of the term ''initially'' and the phrase ''evolve with technological advancements'' in 47 U.S.C. 1422(b) indicate that Congress understood that the definitions of the core network and RAN could not be static. Rather, the definitions of such terms would need to be modified throughout the life of the network in order to help ensure that public safety would have a network capable of supporting and providing access to new and evolving technologies.

Comment #4: Several commenters, although not disagreeing with the proposed definitions, expressed concerns that many of the key elements of the network were either not referenced or did not meet the criteria described in the proposed core network and radio access network definitions. To illustrate this point, multiple commenters reasoned that backhaul transport connecting the radio access network with the core network or the backhaul connecting the core network with geographically distributed databases and application servers, which are critical components of network integration, need to be addressed in the definitions.

Response: FirstNet acknowledges the comments and has modified its interpretation of the ''core network'' to include the Mobility Management Entity within the Evolved Packet Core elements under the 3GPP standards and its interpretation of ''radio access network'' to include backhaul to FirstNet designated consolidation points. To the extent additional clarity is necessary to provide, for example, more specific demarcation points or the services and facilities that will be provided by the various network elements, FirstNet intends to address such matters, as appropriate, in the development of relevant network policies.

2. State Radio Access Networks Must Use the FirstNet Core Network

As discussed above, the Act charges FirstNet with the duty to ''ensure the establishment of a nationwide, interoperable public safety broadband network . . . based on a single, national network architecture'' and defines the architecture of the network as initially consisting of a ''core network'' and a ''radio access network.'' [14] In addition, FirstNet is required to take all actions necessary to ensure the building, deployment, and operation of the network, including issuing RFPs for the purposes of building, operating, and maintaining the network.[15] Thus, overall, FirstNet is responsible for ensuring the core network and radio access network—subject to a State's

[10] *See* 47 U.S.C. 1423(c).

[11] *See id.*

[12] *See* 47 U.S.C. 1442(e)(3)(C)(i).

[13] 47 U.S.C. 1422(b) (emphasis added).

[14] 47 U.S.C. 1422.

[15] 47 U.S.C. 1426(b).

ability to assume RAN responsibilities under 47 U.S.C. 1442—is built, deployed, and operated throughout the country.

As analyzed in the *First Notice,* the Act, although providing each State an opportunity to choose to conduct its own deployment of a RAN in such State, does not provide for State deployment of a core network separate from the core network that FirstNet is charged with deploying.[16] Rather, according to the express language of the Act, FirstNet, is the only entity responsible for constructing a core network. This interpretation is further supported by the mandate that States that choose to build their own RAN must pay any user fees associated with such State's use of ''the core network.'' [17] Thus, based on the language of and overall interoperability goals of the Act, FirstNet makes the following conclusion related to State use of the core network that is constructed, operated, and maintained by FirstNet.

FirstNet concludes that a State choosing to conduct its own deployment of a radio access network under 47 U.S.C. 1442(e) must use the FirstNet core network to provide public safety services within the State.

Analysis of and Responses to Comments to Conclusions That State Radio Access Networks Must Use the FirstNet Core Network

Summary: The majority of commenters agreed with FirstNet's proposed interpretation that a State choosing to conduct its own deployment of a radio access network must use the FirstNet core network to provide services to public safety entities.

Comment #5: One commenter did not support FirstNet's preliminary conclusion, asserting that direct connectivity between the core network and the RAN is excluded from FirstNet's definitions and that such network element should be explicitly identified and included either in the definition of core network or radio access network.

Response: FirstNet acknowledges the comment and notes that, as detailed above, it has clarified the definition of RAN to include backhaul to FirstNet consolidation points.

Comment #6: One commenter agreed with the interpretation, but suggested FirstNet should remain open to the concept of a local ''back-up'' core network, particularly for States or localities with a high population density, with this ''back-up'' core network being designed and purposed to protect against a total loss of connectivity to the FirstNet nationwide core network.

Response: The Act requires FirstNet to establish a network with adequate hardening, security, reliability, and resiliency requirements, including by addressing special considerations for areas and regions with unique homeland security or national security needs.[18] Accordingly, FirstNet intends to construct the core network taking into account these considerations and does not anticipate the need to utilize a local ''back-up'' core network to serve public safety, which, among other things, potentially creates interoperability complexities and increases network security risks.

B. Network Users

1. Final Definition of ''Secondary Users''

The Act in 47 U.S.C. 1428(a)(1) authorizes FirstNet to charge ''user or subscription'' fees to a ''secondary user . . . that seeks access to or use of the [NPSBN].'' Additionally, under 47 U.S.C. 1428(a)(2), FirstNet may enter into a covered leasing agreement with a ''secondary user'' that permits ''access to network capacity on a secondary basis for non-public safety purposes.'' [19] The Act does not expressly define the term ''secondary user.'' However, based on the plain language of 47 U.S.C. 1428, FirstNet reaches the following conclusion with respect to the meaning of ''secondary user'':

FirstNet defines a ''secondary user'' as any user that seeks access to or use of the NPSBN for non-public safety services.

Analysis of and Responses to Comments on Definition of Secondary User

Summary: The majority of commenters agreed with the interpretation of a ''secondary user'' as a user that accesses network capacity on a secondary basis for non-public safety services. One such commenter noted that while secondary users are not public safety entities, they are important to the financial sustainability of the network. Similarly, another commenter remarked that such non-public safety secondary users are necessary to implement a sophisticated and expansive network.

Comment #7: One commenter expressed concern that FirstNet's proposed definition, as formulated, could be misconstrued and sought to clarify that ''secondary user'' captures those using the NPSBN for services that are not related to public safety.

Response: FirstNet has attempted to clearly state in its final definition of ''secondary user'' (identified above) that such term refers to those users who access the NPSBN *only for non-public safety services.*

Comment #8: One commenter expressed concern not about FirstNet's definition of ''secondary user,'' but about the potential for secondary users to adversely impact the performance of the NPSBN at the expense of public safety.

Response: FirstNet is committed to ensuring the establishment of a network that meets the needs of public safety and believes that the 20 MHz of available spectrum along with the expected priority/preemption capabilities of the network will allow secondary users to access the NPSBN without negatively impacting public safety's use of the NPSBN.

Comment #9: One commenter asserted that any user of the NPSBN that is not a ''public safety entity'' should be considered a ''consumer'' rather than a ''secondary user.'' These ''consumers'' would use the network on a secondary basis and yield to the primary user public safety entities.

Response: While FirstNet certainly agrees with the general concept of public safety entities being the primary users of the NPSBN, we do not agree that the term ''consumer'' (which is also undefined in the Act) encompasses all other such users of the network on a secondary basis. First, the Act explicitly uses the term ''secondary user'' when referring to those entities or individuals that access or use the network ''on a secondary basis for non-public safety services.'' [20] Secondly, this use of the term ''consumer'' is inconsistent with 47 U.S.C. 1432, which prohibits FirstNet from providing ''commercial telecommunications or information services directly to consumers.'' Under 47 U.S.C. 1428, FirstNet is expressly authorized to assess a network user fee on secondary users. Thus, given the Act prohibits FirstNet from providing certain services directly to consumers while it permits FirstNet to charge user fees to secondary users, by definition all secondary users cannot be consumers.

2. Prohibition on Providing Commercial Services to Consumers

The Act in 47 U.S.C. 1432(a) specifies that FirstNet ''shall not offer, provide, or market commercial telecommunications or information services directly to consumers.'' The Act does not define

[16] *See* 47 U.S.C. 1422, 1426.

[17] 47 U.S.C. 1442(f).

[18] *See* 47 U.S.C. 1426(b)(2), (c)(2)(A).

[19] 47 U.S.C. 1428(a)(2).

[20] 47 U.S.C. 1428(a).

the word ''consumer'' or indicate whether the word is limited to individuals or includes organizations and businesses. In addition, under the rule of construction specified in 47 U.S.C. 1432(b), nothing in 47 U.S.C. 1432(a) is intended to prohibit FirstNet from entering into covered leasing agreements with secondary users or to limit FirstNet from collecting lease fees for the use of network equipment and infrastructure. FirstNet makes the following conclusions with respect to these provisions of the Act:

(1) The definition of ''consumers'' as used in 47 U.S.C. 1432 does not include:

a. Any public safety entity as defined in the Act;

b. States when seeking access to or use of the core network, equipment, or infrastructure; or

c. entities when seeking access to or use of equipment and infrastructure.

(2) The language of the Act under 47 U.S.C. 1432 prohibiting FirstNet from directly serving ''consumers'' does not limit potential types of public safety entities that may use or access the NPSBN for commercial telecommunications or information services.

(3) The Act under 47 U.S.C. 1432 does not prohibit or act as a limit on secondary users with which FirstNet may enter into a covered leasing agreement.

(4) The Act under 47 U.S.C. 1432 does not limit the pool of secondary users that may gain access to or use of the network on a secondary basis.

Analysis of and Responses to Comments on Prohibition on Providing Commercial Services to Consumers

Summary: The vast majority of commenters supported FirstNet's conclusions that the prohibition in 47 U.S.C. 1432 on FirstNet offering, providing, or marketing commercial telecommunications or information services to consumers does not apply to public safety entities, secondary users, States seeking access to or use of the FirstNet core network, or entities or States seeking access to or use of network equipment and infrastructure. These commenters agreed that the intent of this provision, whether explicit or implicit, is to exclude these entities from the definition of consumer.

Comment #10: One commenter, while not disagreeing with FirstNet's conclusions, expressed concern regarding the potential for network capacity to become saturated from non-public safety use.

Response: As noted above, FirstNet is committed to ensuring the establishment of a network that meets the needs of public safety and believes that the 20 MHz of available spectrum along with the expected priority/preemption capabilities of the network will allow secondary users to access the NPSBN without negatively impacting public safety's use of the NPSBN.

C. Requests for Proposals

1. Requests for Proposals Process

The Act in 47 U.S.C. 1426(b)(1)(B) requires FirstNet to issue ''open, transparent, and competitive'' RFPs. The procedural requirements for issuing such RFPs to meet the ''open, transparent, and competitive'' standard, however, are not defined in the Act. The Federal Acquisition Regulation (''FAR''), codified in 48 CFR parts 1–99, is the primary regulation used by federal executive agencies in their acquisition of supplies and services with appropriated funds. Thus, FirstNet makes the following conclusion with respect to its compliance with this provision:

FirstNet, to the extent it utilizes the FAR, concludes that complying with the FAR satisfies the open, transparent, and competitive requirements of 47 U.S.C. 1426(b)(1)(B).

Analysis of and Responses to Comments on Requests for Proposals

Summary: The overwhelming majority of commenters agreed with FirstNet's proposed interpretation that using the FAR satisfies FirstNet's statutory obligation to issue ''open, transparent, and competitive requests for proposals to private sector entities for the purposes of building, operating, and maintaining the network . . . '' In addition to commenting that compliance with the FAR is a reasonable way of meeting the Act's requirements for an ''open, transparent, and competitive'' RFP process, commenters noted that the FAR is a well understood process, and that by using it, FirstNet will save time by not having to develop a new process for issuing RFPs. Given the size and scope of FirstNet's task, commenters agreed that using the FAR was the most logical option. Some commenters agreed with using the FAR generally, but encouraged the use of only certain sections.

Comment #11: Some commenters suggested that FirstNet exceed the FAR's requirements and reminded FirstNet of its authority to make agreements with States to use existing infrastructure.

Response: FirstNet believes that using the FAR satisfies the Act's requirements. FAR Part 1.102 provides guiding principles of the Federal Acquisition System, namely ''promoting competition, and conducting business with integrity, fairness and openness.'' The policies and procedures of the FAR embody these principles. Adherence to the FAR, therefore, ensures compliance with the Act's mandate to issue ''open, transparent, and competitive'' RFPs. With respect to existing infrastructure, FirstNet plans to leverage such assets for the NPSBN to the extent it is economically desirable, as required by the Act (see below for a further discussion regarding existing infrastructure).

Comment #12: One commenter disagreed with FirstNet's proposed interpretation, observing that the guidance in 47 U.S.C. 1426(b)(1)(B) would be unnecessary if Congress intended FirstNet to comply with the FAR, and that there is not a single reference to the FAR in the Act, despite the extensive statutory guidance the Act provides to FirstNet concerning the RFP process.

Response: FirstNet acknowledges this comment and notes that its final conclusion is *not* that FirstNet believes it is required to use the FAR. Rather, FirstNet's interpretation merely is that by complying with the FAR, FirstNet is complying with this provision of the Act.

2. Minimum Technical Requirements

47 U.S.C. 1426(b)(1)(B) requires FirstNet to issue RFPs for the purposes of building, operating, and maintaining the network that use, *without materially changing,* the minimum technical requirements developed by the Interoperability Board. 47 U.S.C. 1422(b) and 47 U.S.C. 1426(c)(4) further obligate FirstNet to accommodate advancements in technology.[21] With respect to these provisions, FirstNet makes the following final interpretation:

FirstNet concludes that it may make non-material changes or additions/subtractions to the minimal technical requirements developed by the

[21] Note that the Interoperability Board Report states that ''[g]iven that technology evolves rapidly, the network components and associated interfaces identified in the [Interoperability Board Report] . . . are also expected to evolve over time. As such, these aspects of the present document are intended to represent a state-of-the-art snapshot at the time of writing. In this context, the standards, functions, and interfaces referenced in the present document are intended to prescribe statements of intent. Variations or substitutions are expected to accommodate technological evolution consistent with the evolution of 3GPP and other applicable standards.'' Interoperability Board, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network* at 27 (May 22, 2012), *available at http://apps.fcc.gov/ecfs/document/view?id=7021919873.*

Interoperability Board, including as necessary to accommodate advancements in technology as required by the Act.

Analysis of and Responses to Comments on Minimum Technical Requirements

Summary: Commenters were virtually unanimous in agreeing with FirstNet's proposed interpretation regarding changes to the minimum technical requirements established by the Interoperability Board. Several commenters reasoned that such changes are necessary and fully contemplated (by Congress and the Interoperability Board itself) in order to keep pace with evolutions in technology, address issues that the Interoperability Board may not have considered, and fulfill requirements under the Act.

Comment #13: One commenter maintained that the minimum technical requirements developed by the Interoperability Board are so fundamental that they should be utilized in their entirety regardless of advancements in technology.

Response: FirstNet fully appreciates the value of the minimum technical requirements developed by the Interoperability Board and the critical role such requirements will have in the development and maintenance of the NPSBN. However, at the same time, FirstNet seeks to ensure that the most robust and technologically advanced network as possible is established for public safety in accordance with its statutory mission, and FirstNet is specifically directed by the Act to consider advancements in technology in the development and maintenance of the NPSBN.[22] Accordingly, FirstNet intends to operate with those principles and directives in mind in forming the technical requirements for the network.

Comment #14: Multiple commenters urged FirstNet to use open standards in the implementation of advancements in technology, focusing on 3GPP architecture and interfaces that ensure operability, interoperability, and backwards compatibility. Some of these commenters pointed out that the Interoperability Board Report contemplates advancements in technology and supports the open standards process.

Response: This comment is outside the scope of this notice. However, FirstNet acknowledges this recommendation and will consider it as any applicable decisions are developed on the matter. We note that the Act requires that the NPSBN be based on commercial standards, including those developed by 3GPP and that comply with the Interoperability Board Report.

Comment #15: A few commenters suggested that FirstNet rely on the Interoperability Board or a similar independent technical advisory board going forward to establish and maintain ongoing minimum technical requirements and compliance with those requirements, in light of technological advances.

Response: This comment is outside the scope of this notice. However, FirstNet acknowledges this recommendation and will consider it as any applicable decisions are developed on the matter.

Comment #16: Some commenters offered input as to what delineates non-material versus material changes in the minimum technical requirements. Most commenters focused on critical features or functions being backwards compatible, as well as avoiding any reduction in the quality of mission critical service to end users.

Response: FirstNet acknowledges these recommendations and will consider them as any applicable decisions are developed on the matter. FirstNet's goal is to ensure that the NPSBN operates in a manner that satisfies public safety's critical communication needs and is consistent with the material terms of the Interoperability Board report.

3. Final Definition of ''Rural''

The Act directs that FirstNet ''shall require deployment phases with substantial *rural* coverage milestones as part of each phase of the construction and deployment of the network . . . [and] utilize cost-effective opportunities to speed deployment in *rural* areas.'' [23] Additionally, the Act states, in relevant part, that FirstNet ''shall develop . . . requests for proposals with appropriate . . . timetables for construction, including by taking into consideration the time needed to build out to *rural* areas.'' [24] Finally, the Act explains that FirstNet ''shall develop . . . requests for proposals with appropriate . . . coverage areas, including coverage in *rural* and nonurban areas.'' [25]

Since the Act does not define ''rural,'' we found it necessary to define this term in order to fulfill our duties with respect to the above noted statutory rural coverage requirements.[26] Accordingly, FirstNet makes the following final interpretation regarding the definition of ''rural'' under the Act:

(1) FirstNet defines ''rural,'' for the purposes of the Act, as having the same meaning as ''rural area'' in Section 601(b)(3) of the Rural Electrification Act of 1936, as amended (''Rural Electrification Act'' or ''REA''). Section 601(b)(3) of the Rural Electrification Act provides that ''[t]he term 'rural area' means any area other than—(i) an area described in clause (i) or (ii) of Section 1991(a)(13)(A) of this title [section 343(a)(13)(A) of the Consolidated Farm and Rural Development Act]; and (ii) a city, town, or incorporated area that has a population of greater than 20,000 inhabitants.'' In turn, the relevant portion of Section 343(a)(13)(A) of the Consolidated Farm and Rural Development Act explains that the ''terms 'rural' and 'rural area' mean any area other than—(i) a city or town that has a population of greater than 50,000 inhabitants; and (ii) any urbanized area contiguous and adjacent to a city or town described in clause (i).'' Thus, as defined herein, the term ''rural'' means any area that is *not:*

- A city, town, or incorporated area that has a population of greater than 20,000 inhabitants
- any urbanized area contiguous and adjacent to a city or town that has a population of greater than 50,000 inhabitants.

FirstNet also inquired whether there should be a lower boundary separate from the definition of ''rural,'' such as ''wilderness'' or ''frontier.'' Based in part on the comments received, FirstNet has reached the following final conclusion:

(2) FirstNet concludes that a lower boundary (*e.g.,* ''wilderness,'' ''frontier'') is not necessary to satisfy its rural coverage requirements under the Act, and thus FirstNet does *not* intend to establish any such boundary.

[22] *See* 47 U.S.C. 1422(b), 1426(c)(4).

[23] 47 U.S.C. 1426(b)(3) (emphasis added).

[24] 47 U.S.C. 1426(c)(1)(A)(i) (emphasis added).

[25] 47 U.S.C. 1426(c)(1)(A)(ii) (emphasis added).

[26] We appreciate the position the FCC has taken in this regard, and we are committed to fulfill our duties in a way that will meet these rural coverage requirements. *See* Implementing Public Safety Broadband Provisions of the Middle Class Tax Relief and Job Creation Act of 2012 *et al.*, PS Docket 12–94 *et al.*, Notice of Proposed Rulemaking, 28 FCC Rcd 2715, 2728–29 ¶ 46 (2013) (Band 14 NPRM) (noting that, ''We do not believe the Commission should specify rural milestones as a condition of FirstNet's license at this time. Rather, we recognize that at this early stage, the success of FirstNet requires flexibility with respect to deployment and planning, including deployment in rural areas. Moreover, FirstNet has an independent legal obligation under the Act to develop requests for proposals with appropriate timetables for construction, taking into account the time needed to build out in rural areas, and coverage areas, including coverage in rural and nonurban areas. In addition, in light of the Congressional oversight that will be exercised over FirstNet and its other transparency, reporting and consultation obligations, we do not believe it is necessary for the Commission to set specific benchmarks in this regard in these rules.'').

Analysis of and Responses to Comments on Definition of Rural

Summary: Several commenters agreed with FirstNet's proposed definition of ''rural,'' pointing to the logic in using the Rural Electrification Act definition. Many of these commenters noted that the Rural Electrification Act definition is widely known and used. Some specifically agreed that adopting the Rural Electrification Act definition makes sense in light of U.S. Department of Agriculture's (''USDA'') use of the definition in the Rural Broadband Access Loan and Loan Guarantee Program.

However, several other commenters disagreed with FirstNet's proposed definition of rural, suggesting that the Rural Electrification Act definition was inadequate. Multiple commenters expressed concerns that the Rural Electrification Act definition would not accurately measure or reflect the rural areas of a State.

Comment #17: One commenter suggested that the geography of a State could complicate the Rural Electrification Act's application due to many remote, small but densely populated communities and areas without any defined government or established limits.

Response: FirstNet acknowledges this comment and recognizes that certain States may not agree that the Rural Electrification Act definition (or any other definition for that matter) adequately defines rural areas for that State due to unique geographic or other circumstances. However, because FirstNet's mission is to ensure the establishment of a *nationwide* public safety broadband network, it is necessary to formulate a single, objective definition that can be reasonably applied on a national basis. By way of example, the Rural Electrification Act definition of ''rural area'' has been adopted by other federal agencies in determining rural areas on a national basis, including by the USDA in its Rural Broadband Access Loan and Loan Guarantee Program, for application nationwide.[27]

It is also important to note that the primary purpose of the definition of ''rural'' under the Act is to measure whether the statutory requirement to include ''substantial rural coverage milestones'' in each phase of network deployment has been met. The definition does not determine a state or territory's ultimate coverage, which instead will be determined by the input obtained through the consultation process along with FirstNet's available resources.[28]

Comment #18: Some commenters suggested that FirstNet adopt a modified or simplified aggregate population-derived definition utilizing various alternative methodologies. Specifically, a couple of commenters proposed the use of the U.S. Census Bureau's definition of ''rural''—*i.e.,* all areas that are not ''urban areas,'' which consist of Urbanized Areas (50,000 or more people) and Urban Clusters (at least 2,500 and less than 50,000 people).

Response: FirstNet recognizes that there are alternative definitions of ''rural'' utilized by other federal and state government entities and acknowledges that such definitions could be applied in the context of the nationwide public safety broadband network. Consistent with its analysis in the *First Notice,* FirstNet continues to believe, however, that the Rural Electrification Act's definition of ''rural area'' is sufficiently precise to allow for consistent application, as well as widely known and familiar to rural telecommunications providers, rural communities, and other stakeholders considering its utilization specifically with respect to rural broadband issues. In addition, other federal agencies have adopted the Rural Electrification Act definition. The USDA, in particular, utilizes this definition in a similar context through its implementation of the Rural Broadband Access Loan and Loan Guarantee Program, which funds the costs of construction, improvement, and acquisition of facilities and equipment to provide broadband service to eligible rural areas.

Comment #19: Another commenter proposed the adoption of the definition used by USDA's Rural Business Service, indicating that rural areas under such definition are those with 50,000 persons or less excluding areas adjacent to communities larger than 50,000 persons.

Response: See the response to Comment #18 above.

Comment #20: Based on concerns expressed regarding the omission of unincorporated areas and the potential confusion caused by the ''adjacent and contiguous'' clause in the definition, an additional commenter recommended that ''rural'' be defined as a city, town, incorporated area, or unincorporated area that has a population of 20,000 or less.

Response: FirstNet acknowledges the comment. To provide some additional clarity, we note that in identifying cities, towns, incorporated areas, and urbanized areas, FirstNet intends to leverage the U.S. Census definition of ''places,'' which is inclusive of towns, cities, villages, boroughs, and Census Designated Places (CDPs) (which in turn are inclusive, at least in part, of unincorporated areas).[29]

Comment #21: A few commenters advocated for a definition based on population density on a per county basis, with varying formulations. For instance, one such commenter proposed to define rural as a county with a population density of less than 160 persons per square mile, while another commenter proffered any county (i) with a population density of 100 or fewer inhabitants or (ii) of less than 225 square miles. A couple of other commenters suggested using a density of 5/7 to 159 persons per square mile on a county-by-county basis. Similarly, another commenter recommended adopting the definition used by the School-to-Work Opportunities program (*i.e.,* a county, block number area in a nonmetropolitan county, or consortium of counties or such block number areas with a population density of 20 or fewer persons per square mile), reasoning that the definition is simple, from a program with a comparable process and approach (grant eligibility based on an approved State plan, intergovernmental cooperation, seed money for initial planning and development of school-to-work transition system), more objective, and more accurate in identifying rural areas.

Response: See the response to Comment #18 above.

Comment #22: Multiple commenters maintained that instead of adopting the Rural Electrification Act (or any other single definition), the definition of ''rural'' should be determined on a state-by-state basis.

Response: FirstNet recognizes the Act strikes a balance between establishing a nationwide network and providing States an opportunity to make certain decisions about local implementation. As noted above, however, the primary purpose of the definition of ''rural'' is for measuring whether ''substantial rural coverage milestones'' have been included in each phase of deployment, which is required on a national basis. Thus, as a practical matter, there must be a single, uniform, and objective definition of ''rural'' that can be applied nationwide to assess whether such milestones have been met by FirstNet deployment.

[27] The USDA was designated as the lead federal agency for rural development by the Rural Development Policy Act of 1980. *See* 7 U.S.C. 2204b.

[28] *See* 47 U.S.C. 1426(c)(2).

[29] *See* U.S. Census Bureau, *Geographic Terms and Concepts—Place, http://www.census.gov/geo/reference/gtc/gtc_place.html.*

4. Existing Infrastructure

Multiple provisions of the Act direct FirstNet to leverage existing infrastructure when ''economically desirable.'' [30] 47 U.S.C. 1426(b)(1)(C) requires FirstNet in issuing RFPs to ''encourag[e] that such requests leverage, to the maximum extent economically desirable, existing commercial wireless infrastructure to speed deployment of the network.''

Similarly, 47 U.S.C. 1426(b)(3)—in addressing rural coverage and referring to FirstNet's duty and responsibility to issue RFPs—requires that ''[t]o the maximum extent economically desirable, such proposals shall include partnerships with existing commercial mobile providers to utilize cost-effective opportunities to speed deployments in rural areas.''

Finally, 47 U.S.C. 1426(c)(3) requires that in carrying out its various requirements related to the deployment and operation of the NPSBN, ''the First Responder Network Authority shall enter into agreements to utilize, to the maximum extent economically desirable, existing (A) commercial or other communications infrastructure; and (B) Federal, State, tribal, or local infrastructure.'' The Act, however, does not define or establish any criteria for determining economic desirability. FirstNet reaches the following conclusions regarding its obligations to leverage existing infrastructure under 47 U.S.C. 1426:

1. FirstNet interprets that 47 U.S.C. 1426(b)(1)(B) is intended to require FirstNet to encourage, through its requests, that responsive *proposals* leverage existing infrastructure in accordance with the provision.

2. FirstNet interprets 47 U.S.C. 1426(b)(3) as requiring FirstNet to include in its RFPs that such proposals leverage partnerships with commercial mobile providers where economically desirable.

3. FirstNet concludes that factors other than, or in addition to, cost may be utilized in assessing whether existing infrastructure is ''economically desirable,'' including:

a. Infrastructure type/characteristics

b. security (physical, network, cyber, etc.)

c. suitability/viability (ability to readily use, upgrade, and maintain)

d. readiness for reuse (*e.g.,* already in use for wireless communications)

e. scope of use (*e.g.,* range of coverage)

f. availability/accessibility (time/obstacles to acquiring access/use)

g. any use restrictions (*e.g.,* prohibitions/limitations on commercial use)

h. relationships with infrastructure owners/managers (*e.g.,* ease/difficulty in working with owners/managers)

i. available alternatives in the area

Analysis of and Responses to Comments on Leveraging Existing Infrastructure and Economic Desirability

Summary: All commenters on the subject agreed with FirstNet's above interpretations of 47 U.S.C. 1426(b)(1)(C) and (b)(3) that the provisions are intended to require FirstNet to encourage, through its RFPs, that such responsive *proposals* leverage existing infrastructure and partnerships where economically desirable. Many of these commenters emphasized the importance of utilizing the RFP process to leverage existing assets and partnerships to lower costs and increase speed to market.

Comment #23: Some commenters provided input regarding the factors to be considered in making an economic desirability determination, focusing largely on cost.

Response: Although FirstNet agrees that cost is a major factor in assessing economic desirability, we do not believe it is the sole consideration. There are several other factors, as noted above, that are critical to making an informed determination as to whether the infrastructure should be leveraged. For instance, it is essential to understand the infrastructure's suitability for FirstNet's purposes, as well as its availability and readiness for use. Likewise, FirstNet's financial sustainability model is based in large part on its ability to lease excess spectrum capacity to commercial entities for secondary use, and thus consideration of any limitations on commercial use of the infrastructure is imperative.

Comment #24: A couple of commenters suggested other factors besides cost in making an economic desirability determination of whether to leverage infrastructure. One such commenter recommended the consideration of geography and breadth of coverage in addition to cost. Another commenter urged that the requirements of public safety should be considered as a factor.

Response: FirstNet acknowledges these recommendations and believes they are encompassed within FirstNet's final conclusion above regarding economic desirability factors.

D. Fees

FirstNet is required by the Act to be a self-funding entity and has been authorized to assess and collect certain fees for use of the network.[31] Specifically, FirstNet has been authorized to assess and collect a (1) network user fee; (2) lease fee related to network capacity (also known as covered leasing agreement); (3) lease fees related to network equipment and infrastructure; and (4) a fee for State use of elements of the core network.[32] In accordance with these provisions, FirstNet makes the following conclusions related to both the assessment and collection of fees authorized under the Act.

General

(1) FirstNet interprets each of the fees authorized by the Act, including user or subscription fees authorized by 47 U.S.C. 1428(a)(1), covered leasing agreement fees authorized by 47 U.S.C. 1428 (a)(2), lease fees related to network equipment and infrastructure authorized by 47 U.S.C. 1428(a)(3), and the fee for State use of elements of the core network authorized by 47 U.S.C. 1442(f), as distinct and separate from each other and may be assessed individually or cumulatively, as applicable.

Network User Fees

(2) FirstNet concludes it may charge a user or subscription fee under 47 U.S.C. 1428(a)(1) to any user that seeks access to or use of the nationwide public safety broadband network.

State Core Network User Fees

(3) FirstNet concludes that the fees assessed on States assuming RAN responsibilities for use of the core network authorized by 47 U.S.C. 1442(f) are distinct from and can be assessed in addition to any other fees authorized under the Act.

Lease Fees Related to Network Capacity and Covered Leasing Agreements

(4) FirstNet concludes that a covered leasing agreement under 47 U.S.C. 1428(a)(2) does not require a secondary user to ''construct, manage, and operate'' the entire FirstNet network, either from a coverage perspective or exclusively within a specific location.

(5) FirstNet concludes that multiple covered leasing agreement lessees could coexist and be permitted access to excess network capacity in a particular geographic area.

[30] *See* 47 U.S.C. 1426(b)(1)(C), (b)(3), (c)(3).

[31] *See* 47 U.S.C. 1428, 1442(f); 1426(b)(4)(C).

[32] 47 U.S.C. 1428, 1442(f).

(6) FirstNet interprets that a covered leasing agreement lessee satisfies the definition under 47 U.S.C. 1428(a)(2) so long as the lessee does more than a nominal amount of constructing, managing, or operating the network.

(7) FirstNet concludes that an entity entering into a covered leasing agreement under 47 U.S.C. 1428(a)(2) is not required to perform all three functions of constructing, managing, and operating a portion of the network, so long as one of the three is performed as part of the covered leasing agreement.

(8) FirstNet interprets the reference to ''network capacity'' in the definition of covered leasing agreement under 47 U.S.C. 1428(a)(2)(B)(i) as a generic statement referring to the combination of spectrum and network elements, as defined by the Act, and includes the core network as well as the radio access network of either FirstNet alone or that of the secondary user under a covered leasing agreement whereby the core and radio access network are used for serving both FirstNet public safety entities and the secondary user's commercial customers.

(9) FirstNet interprets the term ''secondary basis'' under 47 U.S.C. 1428(a)(2)(B)(i) to mean that network capacity will be available to the secondary user unless it is needed for public safety entities as defined in the Act.

(10) FirstNet interprets the phrase ''spectrum allocated to such entity'' found in 47 U.S.C. 1428(a)(3)(B)(ii) as allowing all or a portion of the spectrum licensed to FirstNet by the FCC under call sign ''WQQE234'' to be allocated for use on a secondary basis under a covered leasing agreement.

(11) FirstNet concludes the reference to ''dark fiber'' in 47 U.S.C. 1428(a)(2)(B)(ii) cannot literally be interpreted as such, and the reference should be interpreted to allow the covered leasing agreement lessee to transport such traffic on otherwise previously dark fiber facilities.

Network Equipment and Infrastructure Fee

(12) FirstNet interprets 47 U.S.C. 1428(a)(3) as being limited to the imposition of a fee for the use of static or isolated equipment or infrastructure, such as antennas or towers, rather than for use of FirstNet spectrum or access to network capacity.

(13) FirstNet interprets the phrase ''constructed or otherwise owned by [FirstNet]'' under 47 U.S.C. 1428(a)(3) as meaning that FirstNet ordered or required the construction of such equipment or infrastructure, paid for such construction, simply owns such equipment, or does not own but, through a contract has rights to sublease access to, or use of, such equipment or infrastructure.

Analysis of and Responses to Comments on Fees

Summary: The majority of commenters agreed with the various interpretations related to the assessment and collection of fees by FirstNet. The commenters generally understood the authority the Act gives FirstNet to assess and collect fees and the importance of such fees as a key funding resource necessary to build, operate, and maintain the NPSBN. However, a few commenters, as described and responded to below, either disagreed with certain interpretations or provided general comments relating to the assessment and collection of the various fees under the Act.

Comment #25: Two commenters agreed that FirstNet is authorized to assess a fee for use of the core network, but suggested that States assuming RAN deployment responsibilities should only pay the costs associated with using the core network and spectrum lease; they should not have to pay a network user or subscription fee, and that FirstNet is not allowed to, or should not, impose 'user' fees on opt-out States in a cumulative manner as interpreted by FirstNet.

Response: FirstNet disagrees and believes the Act authorizes FirstNet to assess a user or subscription fee to each entity, including a State choosing to deploy its own radio access network, that seeks access to or use of the network. Specifically, the Act authorizes FirstNet to collect a ''user or subscription fee from *each* entity, including any public safety entity or secondary user, that seeks access to or use of the [NPSBN].'' [33] Consequently, a plain reading of this provision does not appear to provide any exclusionary language that would limit which entities may be charged a fee for access to or use of the network. Rather, as discussed in the *First Notice,* the use of the term ''including'' rather than ''consisting'' when describing the scope of entities that may be charged a network user fee indicates that this group is not limited to only public safety entities or secondary users, but would include other entities such as a State. Thus, FirstNet believes the plain language of the Act supports the conclusion that FirstNet may charge a user or subscription fee to *any* eligible user who seeks access to or use of the nationwide public safety broadband network, including, as appropriate, a State assuming responsibilities for radio access network deployment.

Comment #26: One commenter suggested that all public safety user fees should include nationwide coverage, and should be for unlimited use of the NPSBN. For example, a flat fee for unlimited usage (and no roaming fees) should be charged within each State, similar to today's carrier billing model.

Response: This comment is outside the scope of this notice. However, FirstNet acknowledges the comment and will consider the recommendation as it continues planning for the deployment of the NPSBN.

Comment #27: One commenter suggested that while the Act is unambiguous on allowing FirstNet to assess a fee to States assuming RAN responsibilities for use of the core network, it is important that this fee not be set so high so as to discourage States from opting out of the NPSBN. The commenter further noted that the ability of States to construct their own RAN is clearly permissive under the Act and, in fact, could enable significant growth and adoption of the NPSBN as long as the user fees for opt-out states are reasonable and contemplate the budgets of State and local public safety entities.

Response: This comment is outside the scope of this notice. However, FirstNet acknowledges the comment and will consider the recommendation as it continues planning for the deployment of the NPSBN.

Comment #28: Two commenters disagreed that ''all'' of the FirstNet Band 14 spectrum can be allocated for secondary use under a covered leasing agreement.

Response: FirstNet believes its interpretation that the Act allows all or part of the spectrum licensed to FirstNet by the FCC under call sign ''WQQE234'' to be allocated for secondary use is supported by language of the Act. FirstNet is the entity created by the Act to ensure the establishment of the NPSBN, and as such has a duty to ensure the efficient use of the funding resources available to fulfill this duty, including the ability to permit access to spectrum capacity on a secondary basis. To best utilize these funding resources, the Act authorizes FirstNet to enter into covered leasing agreements which permit an entity entering into such an agreement to have access to, or use of, network capacity on a secondary basis for non-public safety services. The Act, as analyzed in the *First Notice,* does not provide any cap or limitation on how much of the network capacity may be allocated on a secondary basis. Thus, FirstNet believes the Act provides it

[33] 47 U.S.C. 1428(a)(1) (emphasis added).

flexibility to determine how best to utilize network capacity as a funding resource to ensure both the establishment and self-sustainability of the network. Despite this flexibility, however, it is important to note that public safety entities will always have priority use of the NPSBN over any non-public safety user that gains access to, or use of, the network on a secondary basis.

Comment #29: One commenter suggested that the States should determine how much capacity/spectrum is made available within its borders under a covered leasing agreement—rather than FirstNet making the determination.

Response: FirstNet is the entity created by the Act to ensure the establishment of the NPSBN and is also the sole licensee of the 700 MHz D block spectrum and the existing public safety broadband spectrum.[34] Thus, FirstNet is the sole entity responsible for determining how to allocate the spectrum under a covered leasing agreement.

Comment #30: One commenter cautioned FirstNet to ensure there is not an undue expectation by the covered leasing agreement lessee that its lease of the spectrum supersedes public safety's access to, and use of, that spectrum as a priority in all cases, and at all times.

Response: FirstNet acknowledges the comment and reiterates that its primary mission is to ensure the establishment of a nationwide, interoperable network for public safety. Accordingly, public safety will always have priority use of the NPSBN over any non-public safety user that gains access to, or use of, the network on a secondary basis through a covered leasing agreement.

Comment #31: One commenter recommended that FirstNet interpret 47 U.S.C. § 1428(a)(3) to only apply to the RAN hardware in States that choose to participate in the NPSBN as proposed by FirstNet.

Response: FirstNet interprets the phrase ''constructed or otherwise owned by [FirstNet]'' under 47 U.S.C. 1428(a)(3) as meaning that FirstNet ordered or required the construction of such equipment or infrastructure, paid for the construction, owns the equipment, or does not own the equipment, but, through a contract, has the right to sublease the equipment or infrastructure. Thus, unless the RAN hardware in any State falls within the criteria above, FirstNet would not have the authority to assess and collect a fee for use of such infrastructure or equipment.

[34] 47 U.S.C. 1421, 1422.

Dated: October 15, 2015.

Jason Karp,

Chief Counsel (Acting), First Responder Network Authority.

[FR Doc. 2015–26621 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–TL–P

DEPARTMENT OF COMMERCE

Foreign-Trade Zones Board

[S–134–2015]

Foreign-Trade Zone 142—Salem/Millville, New Jersey; Application for Subzone; Nine West Holdings, Inc.; West Deptford, New Jersey

An application has been submitted to the Foreign-Trade Zones (FTZ) Board by the South Jersey Port Corporation, grantee of FTZ 142, requesting subzone status for the facilities of Nine West Holdings, Inc., located in West Deptford, New Jersey. The application was submitted pursuant to the provisions of the Foreign-Trade Zones Act, as amended (19 U.S.C. 81a–81u), and the regulations of the FTZ Board (15 CFR part 400). It was formally docketed on October 14, 2015.

The proposed subzone would consist of the following sites: *Site 1* (27.18 acres) 1245 Forest Parkway West, West Deptford; and, *Site 2* (33.28 acres) 1250 Parkway West, West Deptford. The proposed subzone would be subject to the existing activation limit of FTZ 142. No authorization for production activity has been requested at this time.

In accordance with the FTZ Board's regulations, Kathleen Boyce of the FTZ Staff is designated examiner to review the application and make recommendations to the Executive Secretary.

Public comment is invited from interested parties. Submissions shall be addressed to the FTZ Board's Executive Secretary at the address below. The closing period for their receipt is November 30, 2015. Rebuttal comments in response to material submitted during the foregoing period may be submitted during the subsequent 15-day period to December 14, 2015.

A copy of the application will be available for public inspection at the Office of the Executive Secretary, Foreign-Trade Zones Board, Room 21013, U.S. Department of Commerce, 1401 Constitution Avenue NW., Washington, DC 20230–0002, and in the ''Reading Room'' section of the FTZ Board's Web site, which is accessible via *www.trade.gov/ftz*.

For further information, contact Kathleen Boyce at *Kathleen.Boyce@trade.gov* or (202) 482–1346.

Dated: October 14, 2015.

Andrew McGilvray,

Executive Secretary.

[FR Doc. 2015–26632 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

Foreign-Trade Zones Board

[B–67–2015]

Foreign-Trade Zone (FTZ) 183—Austin, Texas; Notification of Proposed Production Activity; Flextronics America, LLC (Automatic Data Processing Machines); Austin, Texas

Flextronics America, LLC (Flextronics) submitted a notification of proposed production activity to the FTZ Board for its facility in Austin, Texas within Subzone 183C. The notification conforming to the requirements of the regulations of the FTZ Board (15 CFR 400.22) was received on October 9, 2015.

Flextronics already has authority to produce automatic data processing machines within Subzone 183C. The current request would add finished products and foreign status materials/components to the scope of authority. Pursuant to 15 CFR 400.14(b), additional FTZ authority would be limited to the specific foreign-status materials/components and specific finished products described in the submitted notification (as described below) and subsequently authorized by the FTZ Board.

Production under FTZ procedures could exempt Flextronics from customs duty payments on the foreign status materials/components used in export production. On its domestic sales, Flextronics would be able to choose the duty rates during customs entry procedures that apply to: Video card subassemblies; CPU and video card connector subassemblies; external power and USB port card subassemblies; main controller board subassemblies; and, internal power supply subassemblies (duty-free) for the foreign status materials/components noted below and in the existing scope of authority. Customs duties also could possibly be deferred or reduced on foreign status production equipment.

The materials/components sourced from abroad include: Copper alloy screws; and, lithium batteries (duty rate ranges from 3.0 to 3.4%).

Public comment is invited from interested parties. Submissions shall be addressed to the Board's Executive Secretary at the address below. The

Final Interpretation—2nd Notice

FirstNet provided their final interpretation on the second notice which focused on the following items:

- **Technical requirements for equipment to be used on the network, including open standards for connectivity and device competition**
    - *Promoting competition in the equipment marketplace:*
        - *Applies to any equipment used 'on' the network, but does not include equipment that is used to constitute the network*
        - *Applies only to those parameters necessary to maintain interoperability with the NPSBN*
        - *Applies either access is through FirstNet-deployed RAN or State-deployed RAN*

    Florida agrees but sought further clarification regarding which entity will be responsible for standards after the NPSBN implementation, how 'capable' should be determined through a certification process

- **The nature and application of FirstNet network policies, including those that aim to preserve interoperability in states and territories that assume responsibility for building and operation of the RAN**
    - *Applies to all elements of the network, whether FirstNet-deployed or State-deployed*
    - *A State's demonstration of interoperability to FCC/NTIA is a commitment to FirstNet's network policies*
    - *FirstNet could require compliance with policies as a condition of entering into a spectrum capacity lease pursuant*

    Florida maintains that the network policies should be shaped by States, Tribes and public safety partners, and may be informed by private partners

- **The state/territory decision regarding assumption of the responsibility to build and operate a RAN, related approval processes and standards, and the roles and responsibilities of states throughout the process**
    - *Governor's decision is binding on all jurisdictions within the State*

    Florida recognized that the Florida Tribes might have a different decision than the Governor

    FirstNet continues to seek guidance from the Act and tribal jurisdictions. There is a potential that FirstNet and the Tribes will work directly with each other.

    Florida encourages FirstNet to find opportunities to share information to inform the State plan

    FirstNet plans to coordinate through consultations the details of the proposed State plan when they are available

    - *FirstNet and the State can work together to permit added components beyond the State plan*
    - *Notice to opt-in can either be in writing or not, provided to FirstNet, NTIA, and FCC in the same day*
    - *'Complete request for proposals' - a State has progressed to the extent necessary to*

submit an alternative plan

- *'Completion of the RFP process' - not defined in the Act; when FirstNet obtains sufficient amount of information to present a State plan; plans will/could be presented at different times for different states*

Florida suggested that FirstNet provide the minimum legally required contents of the State plan to the states so they could understand the benchmarks

FirstNet disagreed and said the Act does not require that

Florida encouraged an extension to the 180-day timeline to produce an alternative plan

FirstNet had no ability to change the Act and cannot extend the time

- **Customer, operational, and funding considerations regarding state/territory assumption of the responsibility to build and operate a RAN**
  - *Must meet interoperability and self-sustainment goals of the Act*
  - *States not required to be public-facing entity*

as pay adjustments, bonuses and Presidential Rank Awards for SES members. The appointment of these members to the Performance Review Board will be for a period of twenty-four (24) months.

DATES: The period of appointment for those individuals selected for EDA's Performance Review Board begins on October 20, 2015. The name, position title, and type of appointment of each member of EDA's Performance Review Board are set forth below by organization:

1. *Department of Commerce, Office of the Secretary, Office of the General Counsel (OS/OGC)*
   Stephen D. Kong, Chief Counsel for Economic Development, Career SES, Chairperson
2. *Department of Commerce, Minority Business Development Agency (MBDA)*
   Edith J. McCloud, Associate Director for Management, Career SES
3. *Department of Commerce, Office of the Secretary (OS), Office of the Chief Financial Officer and Assistant Secretary for Administration (CFO/ASA)*
   Renee A. Macklin, Director for Program Evaluation and Risk Management, Career SES (New Member)
4. *Department of Commerce, National Oceanic and Atmospheric Administration (NOAA)*
   Russell F. Smith, III, Deputy Assistant Secretary for International Fisheries, Non-Career SES

Denise A. Yaag,

Director, Office of Executive Resources, Office of Human Resources Management, Office of the Secretary/Office of the CFO/ASA, Department of Commerce.

[FR Doc. 2015–26582 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–25–P

DEPARTMENT OF COMMERCE

Economics and Statistics Administration

Performance Review Board Membership

AGENCY: Economics and Statistics Administration, Department of Commerce.

ACTION: Notice.

SUMMARY: Below is a listing of individuals who are eligible to serve on the Performance Review Board (PRB) in accordance with the Economics and Statistics Administration's (ESA) Senior Executive Service and Senior Professional performance management systems:

Kenneth A. Arnold, Deputy Under Secretary for Economic Affairs, ESA
Lisa M. Blumerman, Associate Director for Decennial Census Programs, Census Bureau
William G. Bostic, Jr., Associate Director for Economic Programs, Census Bureau
Stephen B. Burke, Chief Financial Officer and Director for Administration, ESA
Joanne Buenzli Crane, Associate Director for Administration and Chief Financial Officer, Census Bureau
Austin J. Durrer, Chief of Staff, ESA
Susan Helper, Special Advisor, ESA
Ron S. Jarmin, Assistant Director for Research and Methodology, Census Bureau
Enrique Lamas, Associate Director for Demographic Programs, Census Bureau
Harry Lee, Assistant Director for Information Technology and Deputy Chief Information Officer, Census Bureau
Thomas A. Louis, Associate Director for Research and Methodology, Census Bureau
Jennifer Madans, Associate Director for Science, Center for Disease Control and Prevention
Brent R. Moulton, Associate Director for National Economics, Bureau of Economic Analysis
Brian C. Moyer, Director, Bureau of Economic Analysis
Joel D. Platt, Associate Director for Regional Economics, Bureau of Economic Analysis
Nancy A. Potok, Deputy Director, Census Bureau
Pravina A. Raghavan, Senior Advisor for Policy and Program Integration, Office of the Deputy Secretary
Angela Simpson, Deputy Assistant Secretary for Communications and Information, National Telecommunications and Information Administration
Jeannie L. Shiffer, Associate Director for Communications, Census Bureau
Sarahelen Thompson, Associate Director for International Economics, Bureau of Economic Analysis
Katherine K. Wallman, Chief Statistician, Office of Management and Budget

The purpose of a PRB is to provide fair and impartial review of recommended SES/ST performance ratings, bonuses, and pay adjustments and Presidential Rank Award nominations. The term of each PRB member will expire on December 31, 2017.

FOR FURTHER INFORMATION CONTACT: Latasha Ellis, Executive Resources Office, 301–763–3727.

Dated: October 12, 2015.

Stephen B. Burke,

Chief Financial Officer and Director for Administration, Chair, ESA Performance Review Board.

[FR Doc. 2015–26586 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–BS–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

First Responder Network Authority

[Docket Number: 140821696–5909–05]

RIN 0660–XC012

Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012

AGENCY: First Responder Network Authority, National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice; final interpretations.

SUMMARY: The First Responder Network Authority (''FirstNet'') publishes this *Notice* to issue final interpretations of its enabling legislation that will inform, among other things, forthcoming requests for proposals, interpretive rules, and network policies. The purpose of this Notice is to provide stakeholders FirstNet's interpretations on many of the key preliminary interpretations presented in the proposed interpretations published on March 13, 2015.

DATES: Effective October 20, 2015.

FOR FURTHER INFORMATION CONTACT: Eli Veenendaal, First Responder Network Authority, National Telecommunications and Information Administration, U.S. Department of Commerce, 12201 Sunrise Valley Drive, M/S 243, Reston, VA 20192; 703–648–4167; or *elijah.veenendaal@firstnet.gov.*

SUPPLEMENTARY INFORMATION:

I. Introduction and Background

The Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112–96, Title VI, 126 Stat. 256 (codified at 47 U.S.C. 1401 *et seq.*)) (the ''Act'') established the First Responder Network Authority (''FirstNet'') as an independent authority within the National Telecommunications and Information Administration (''NTIA''). The Act establishes FirstNet's duty and responsibility to take all actions necessary to ensure the building, deployment, and operation of a nationwide public safety broadband network (''NPSBN'').[1]

One of FirstNet's initial steps in carrying out this responsibility pursuant to the Act is the issuance of open, transparent, and competitive requests for proposals (''RFPs'') for the purposes of building, operating, and maintaining

[1] 47 U.S.C. 1426(b).

the network. We have sought, and may continue to seek, public comments on many technical and economic aspects of these RFPs through traditional procurement processes, including requests for information (''RFIs'') and potential draft RFPs and Special Notices, prior to issuance of RFPs.[2]

As a newly created entity, however, we are also confronted with many complex legal issues of first impression pursuant to the Act that will have a material impact on the RFPs, responsive proposals, and our operations going forward. Generally, the Administrative Procedure Act (''APA'')[3] provides the basic framework of administrative law governing agency action, including the procedural steps that must precede the effective promulgation, amendment, or repeal of a rule by a federal agency.[4] However, section 1426(d)(2) of the Act provides that any action taken or decision made by FirstNet is exempt from the requirements of the APA.[5]

Nevertheless, although excluded from these procedural requirements, on March 13, 2015, FirstNet published a public notice entitled ''Further Proposed Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012'' (hereinafter ''the Second Notice''),[6] seeking public comments on preliminary interpretations on certain foundational legal issues, as well as technical and economic issues, to help guide FirstNet's efforts in achieving its mission.

The purpose of this *Notice* is to provide stakeholders notice of the final legal interpretations on many of the key preliminary interpretations presented in the *Second Notice*. Additional background, rationale for this action, and explanations of FirstNet's interpretations were included in the *Second Notice* and are not repeated herein. The section immediately below labeled ''Final Interpretations'' summarizes FirstNet's final interpretations with respect to the *Second Notice*. Thereafter, the section labeled ''Response to Comments'' summarizes the comments received on the preliminary interpretations contained in the *Second Notice* and provides FirstNet's responses to such comments, including further explanations to FirstNet's interpretations.

II. Final Interpretations

In sum, FirstNet makes the following final interpretations related to topics in the *Second Notice:*

A. Technical Requirements Relating to Equipment for Use on the NPSBN

Promoting Competition in the Equipment Market Place

1. FirstNet interprets 47 U.S.C. 1426(b)(2)(B) as applying to any equipment, including end user devices, used ''on'' (*i.e.,* to use or access) the network, but does not include any equipment that is used to constitute the network (*i.e.,* the core network or radio access network (''RAN'')).

2. FirstNet concludes that the Act's goal of ''promot[ing] competition in the equipment market'' is satisfied by applying the requirements listed in 47 U.S.C. 1426(b)(2)(B)(i) to only those parameters necessary to maintain interoperability (*i.e.,* ''connectivity'') with the NPSBN, which are included in the Interoperability Board Report or otherwise in FirstNet network policies.

3. FirstNet concludes that 47 U.S.C. 1426(b)(2)(B) applies regardless of whether the equipment will access or use the NPSBN via a FirstNet-deployed RAN or a State-deployed RAN.

B. FirstNet Network Policies

Network Policies

4. FirstNet concludes that the items listed in 47 U.S.C. 1426(c)(1)(A) relating to RFPs are ''policies'' for purposes of 47 U.S.C. 1426(c)(2) and as the term is generally used in 47 U.S.C. 1426(c).

5. FirstNet concludes that the network policies developed pursuant to 47 U.S.C. 1426(c)(1) apply to all elements of the network, including RANs deployed by individual States pursuant to 47 U.S.C. 1442(e)(3).

6. FirstNet concludes that a required aspect of a State's demonstrations of interoperability to both the Federal Communications Commission (''FCC'') and NTIA under 47 U.S.C. 1442(e)(3), is a commitment to adhering to FirstNet's network policies implemented under 47 U.S.C. 1426(c).

7. FirstNet concludes that it could require compliance with network policies essential to the deployment and interoperable operation of the network for public safety in all States as a condition of entering into a spectrum capacity lease pursuant to 47 U.S.C. 1442(e)(3)(C)(iii)(II).

C. A State's Opportunity To Assume Responsibility for RAN Deployment and Operation

Final Interpretations Regarding the Presentation of a State Plan and the Completion of Request for Proposal Process

8. FirstNet interprets 47 U.S.C. 1442(e) to merely require completion of the request for proposal process for the State in question, rather than the nation as a whole, prior to presentation of the plan to the State, assuming that FirstNet can at that stage otherwise meet the requirements for presenting a plan (and its contents) to such State.

9. FirstNet concludes that ''completion'' of the request for proposal process occurs when FirstNet has obtained sufficient information to present the State plan with the details required pursuant to the Act for such plan, but not necessarily at any final award stage of such a process.

Final Interpretations Regarding the Content of a State Plan

10. FirstNet concludes that the details of the proposed State plan pursuant to 47 U.S.C. 1442(e)(1)(B) should include at least certain outcomes of the RFP process.

11. FirstNet concludes that the FirstNet plan must contain sufficient information to enable NTIA to make comparisons of cost-effectiveness, security, coverage, and quality of service.

Governor's Role in the State Plan Process

12. FirstNet concludes that the decision of the Governor pursuant to 47 U.S.C. 1442(e)(2), for purposes of the Act, is binding on all jurisdictions within such State, and that such a decision must be made for the entire State, and not simply a subset of individual jurisdictions within such State.

13. FirstNet concludes that FirstNet and a State could agree that FirstNet and the State (or sub-State jurisdictions) work together to permit implementation of added RAN coverage, capacity, or other network components beyond the State plan to the extent the interoperability, quality of service, and other goals of the Act are met.

[2] The pronouns ''we'' or ''our'' throughout this *Notice* refer to ''FirstNet'' alone and not FirstNet, NTIA, and the U.S. Department of Commerce as a collective group.

[3] *See* 5 U.S.C. 551–59, 701–06, 1305, 3105, 3344, 5372, 7521.

[4] *See* 5 U.S.C. 551–559. The APA defines a ''rule'' as ''the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency and includes the approval or prescription for the future of rates, wages, corporate or financial structures or reorganizations thereof, prices, facilities, appliances, services or allowances therefor or of valuations, costs, or accounting, or practices bearing on any of the foregoing.'' 5 U.S.C. 551(4).

[5] 47 U.S.C. 1426(d)(2).

[6] 80 FR 13336 (Mar. 13, 2015).

Final Interpretations Regarding the Timing and Nature of a State's Decision

14. FirstNet concludes that the Governor must await notice and presentation of the FirstNet plan prior to making the decision pursuant to 47 U.S.C. 1442(e)(2).

15. FirstNet concludes that a State decision to participate in the FirstNet proposed deployment of the network in such State may be manifested by a State providing either (1) actual notice in writing to FirstNet within the 90-day decision period or (2) no notice within the 90-day period established pursuant to 47 U.S.C. 1442(e)(2).

16. FirstNet interprets the requirement within 47 U.S.C. 1442(e)(3) stating that the notice is to be provided to FirstNet, NTIA, and the FCC as being a contemporaneous (*i.e.,* same day) requirement.

The Nature of FirstNet's Proposed State Plan

17. FirstNet concludes that the presentation of a plan to a Governor and his/her decision to either participate in FirstNet's deployment or follow the necessary steps to build a State RAN does not create a contractual relationship between FirstNet and the State.

Final Interpretations Regarding the State's Development of an Alternative Plan

18. FirstNet concludes that the phrase ''complete requests for proposals'' means that a State has progressed in such a process to the extent necessary to submit an alternative plan for the construction, maintenance, operation, and improvements of the RAN, that demonstrates the technical and interoperability requirements in accordance with 47 U.S.C. 1442(e)(3)(C)(i).

19. FirstNet concludes that where a State fails to ''complete'' its request for proposal within the 180-day period pursuant to the Act, the State forfeits its ability to submit an alternative plan pursuant to 47 U.S.C. 1442(e)(3)(C), and the construction, maintenance, operations, and improvements of the RAN within the State shall proceed in accordance with the FirstNet proposed plan for such State.

Final Interpretations Regarding the Responsibilities of FirstNet and a State Upon a State Decision To Assume Responsibility for the Construction and Operation of Its Own RAN

20. FirstNet concludes that once a plan has been disapproved by the FCC, subject only to the additional review described in 47 U.S.C. 1442(h), the opportunity for a State to conduct its own RAN deployment pursuant to 47 U.S.C. 1442(e)(3) will be forfeited, and FirstNet shall proceed in accordance with its proposed plan for that State.

21. FirstNet concludes, following an FCC-approved alternative State RAN plan, it would have no obligation to construct, operate, maintain, or improve the RAN within such State.

22. FirstNet concludes that if a State, following FCC approval of its alternative plan, is unable or unwilling to implement its alternative plan in accordance with all applicable requirements, then FirstNet may assume, without obligation, RAN responsibilities in the State.

D. Customer, Operational and Funding Considerations Regarding State Assumption of RAN Construction and Operation

Customer Relationships in States Assuming RAN Construction and Operation

23. FirstNet concludes that the Act provides sufficient flexibility to accommodate many types of customer relationships with public safety entities for States assuming RAN responsibility so long as the relationships meet the interoperability and self-sustainment goals of the Act.

24. FirstNet concludes that the Act does not require that States assuming RAN deployment responsibilities be the customer-facing entity entering into agreements with and charging fees to public safety entities in such States.

25. FirstNet concludes that the Act does not preclude States assuming RAN deployment responsibilities from charging subscription fees to public safety entities if FirstNet and such States agree to such an arrangement in the spectrum capacity lease.

26. FirstNet concludes that the Act provides sufficient flexibility to allow the determination of whether FirstNet or a State plays a customer-facing role to public safety entities in a State assuming RAN responsibilities to be the subject of operational discussions between FirstNet and the State in negotiating the terms of the spectrum capacity lease.

27. FirstNet concludes that it will maintain a flexible approach to such functions and interactions in order to provide the best solutions to each State so long as the agreed upon approach meets the interoperability and self-sustainment goals of the Act.

Final Interpretation of FirstNet Analyzing Funding Considerations as Part of Its Determination To Enter Into a Spectrum Capacity Lease

28. FirstNet concludes, in fulfilling its duties and responsibilities pursuant to the Act, it can and must take into account funding considerations, including the ''cost-effectiveness'' of an alternative state plan as it may impact the national deployment of the NPSBN, in determining whether and under what terms to enter into a spectrum capacity lease with a State.[7]

29. FirstNet concludes as part of its cost-effectiveness analysis in determining whether and under what terms to enter into a spectrum capacity lease, it (i) must consider the impact of cost-inefficient alternative RAN plans, including inefficient use of scarce spectrum resources, on the NPSBN, and (ii) may require that amounts generated within a State in excess of those required to reasonably sustain the State RAN, be utilized to support the Act's requirement to deploy the NPSBN on a nationwide basis.

30. FirstNet concludes as part of its cost-effectiveness analysis, it must consider State reinvestment and distribution of any user fees assessed to public safety entities or spectrum capacity revenues in determining whether and under what terms to enter into a spectrum capacity lease.

Reinvestment of User or Subscriber Fees

31. FirstNet concludes that the Act requires that States assuming RAN deployment responsibilities and charging user or subscription fees to public safety entities must reinvest such fees into the network.

32. FirstNet concludes it could impose a reinvestment restriction within the terms of a spectrum capacity lease with a State.

Reinvestment of Revenues From State Covered Leasing Agreements/Public-Private Partnerships

33. FirstNet concludes that, in practical effect, the literal statutory differences between a covered leasing agreement and public-private partnership as used in the Act result in no substantive difference between the Act's treatment of FirstNet and States that assume RAN responsibility.

34. FirstNet concludes that any revenues from public-private partnerships, to the extent such arrangements are permitted and different than covered leasing agreements, should be reinvested into the network and that the reinvestment

[7] *See* 47 U.S.C. 1442(e)(3)(D).

provision of 47 U.S.C. 1442(g) should be interpreted to require such reinvestment.

III. Response to Comments

FirstNet received 70 written comments in response to the *Second Notice* from various stakeholders, including States, tribes, public safety organizations, commercial carriers, equipment vendors, utilities, and various associations. Comments included the submission of a large number of identical or similar comments as well as oral statements made during meetings with FirstNet. FirstNet has carefully considered each of the comments submitted. FirstNet has grouped and summarized the comments according to common themes and has responded accordingly. All written comments can be found at *www.regulations.gov.*

A. Final Interpretations of Technical Requirements Relating to Equipment for Use on the NSPBN

Promoting Competition in the Equipment Market Place

The Act requires FirstNet to ''promote competition in the equipment market, including devices for public safety communications, by requiring that equipment for use on the network be: (i) Built to open, non-proprietary, commercially available standards; (ii) capable of being used by any public safety entity and by multiple vendors across all public safety broadband networks operating in the 700 MHz band; and (iii) backward-compatible with existing commercial networks to the extent that such capabilities are necessary and technically and economically reasonable.'' [8] Given the interoperability goals of the Act, and the fact that end user devices will need to operate seamlessly across the network regardless of State decisions to assume RAN responsibilities, FirstNet makes the following final interpretations related to this provision:

1. FirstNet interprets 47 U.S.C. 1426(b)(2)(B) as applying to any equipment, including end user devices, used ''on'' (*i.e.,* to use or access) the network, but does not include any equipment that is used to constitute the network (*i.e.,* the core network or RAN).

2. FirstNet concludes that the Act's goal of ''promot[ing] competition in the equipment market'' is satisfied by applying the requirements listed in 47 U.S.C. 1426(b)(2)(B)(i) to only those parameters necessary to maintain interoperability (*i.e.,* ''connectivity'') with the NPSBN, which are included in the Interoperability Board Report or otherwise in FirstNet network policies.

3. FirstNet concludes that 47 U.S.C. 1426(b)(2)(B) applies whether or not the equipment is to access or use the NPSBN via a FirstNet-deployed RAN or a State-deployed RAN.

Analysis of and Responses to Comments on Technical Requirements Relating to Equipment for Use on the NPSBN

Summary: The majority of commenters supported FirstNet's proposed interpretations regarding technical requirements relating to equipment for use on the NPSBN, emphasizing, for example, that a contrary interpretation could lead to incompatible equipment, thereby limiting interoperability and resulting in higher-priced end user equipment. In particular, all commenters agreed that 47 U.S.C. 1426(b)(2)(B) applies regardless of whether the equipment will access or use the NPSBN via a FirstNet-deployed RAN or a State-deployed RAN. Interoperability of end-user devices across the entire network was the primary basis for this perspective. As documented below, however, certain commenters disagreed or provided general comments on these interpretations.

Comment #1: Several commenters stated the FirstNet proposed interpretation limiting the applicability of 47 U.S.C. 1426(b)(2)(B) to subscriber equipment (*i.e.,* end-user devices) only and not system infrastructure (*i.e.,* the core network and RAN) is not supported by the plain language of the Act and should be interpreted to apply more broadly to all network equipment and infrastructure.

Response: FirstNet disagrees that its interpretation is not supported by the plain language of the Act or should be applied more broadly to include network components or equipment (*i.e.,* the core network and RAN). First, there is nothing in 47 U.S.C. 1426(b)(2)(B) that directly indicates or references equipment or components constituting the core network or RAN. Rather, the Act expressly states that 47 U.S.C. 1426(b)(2)(B) applies only to equipment ''for use on'' the NPSBN, rather than, for example, ''equipment of'' or ''equipment constituting'' the NPSBN. More specifically, the Act states that the range of equipment implicated in this provision must at least include ''devices,'' which, in the telecommunications market, is often a reference to end user devices, rather than equipment used inside the network to provide service to such devices.[9]

Second, the Act provides a separate standard when discussing equipment constituting the NPSBN versus equipment for use on the network. In particular, the *network components* of the NPSBN itself initially consists of a core network and RAN, both of which are required to be based on ''commercial standards.'' [10] Conversely, when describing *equipment,* the Act requires that such equipment must be built not only to commercial standards, but also to ''open, non-proprietary'' standards.[11] Consequently, a plain reading of the Act indicates that Congress intended for different standards to apply to the network components (*i.e.,* core network and RAN) and equipment for use on the network described in 47 U.S.C. 1426(b)(2)(B).

Finally, this interpretation is supported by the other two elements appearing in 47 U.S.C. 1426(b)(2)(B). For example, 47 U.S.C. 1426(b)(2)(B)(ii) requires that such equipment be ''capable of being used by any public safety entity,'' which would seem inconsistent with a requirement applicable to complex network routing and other equipment used inside the network. Similarly, 47 U.S.C. 1426(b)(2)(B)(iii) requires such equipment to be ''backward-compatible with existing commercial networks'' in certain circumstances, which would again make sense in the context of end user devices, but not equipment being used to construct the network. Thus, based on the analysis in the *Second Notice* and supporting comments, FirstNet interprets the plain language of the Act describing equipment in 47 U.S.C. 1426(b)(2)(B) as referring to equipment using the services of the network, rather than equipment forming elements of the NPSBN (*i.e.,* core network or the RAN).

Comment #2: One commenter stated that it is critical for FirstNet to understand that a paramount concern of the Act is to avoid a replication of the underlying conditions that led to limited participants in the public safety ecosystem, including the use of equipment that is not based on generally accepted commercial standards, but were in fact proprietary technologies that were, in most cases by design, not interoperable with other commercially available alternatives, resulting in limited competition and increased costs.

Response: FirstNet acknowledges the comment and understands the

[8] 47 U.S.C. 1426(b)(2)(B)(i).

[9] *See* 47 U.S.C. 1426(b)(2)(B).

[10] *See* 47 U.S.C. 1422(b).

[11] *See* 47 U.S.C. 1426(b).

importance of promoting competition in the equipment marketplace as described in 47 U.S.C. 1426(b)(2)(B), while at the same time allowing for the development of innovative technologies that will interoperate with the NPSBN and provide the best solutions for public safety.

Comment #3: A few commenters disagreed with the interpretation and suggested further clarity was required around the specific elements that constitute the FirstNet core network and RAN in order to better understand the scope of the proposed interpretation.

Response: FirstNet refers the commenters to the final interpretations to the *First Notice,*[12] which discuss in detail the specific elements that constitute the FirstNet core network and RAN.

Comment #4: One commenter encouraged FirstNet to focus on optimizing options, rather than defining network openness proscriptively. The commenter reasoned that FirstNet should take into consideration the fact that maximizing customer choice and vendor competition on handsets will also require an eye towards RAN equipment open standards to maximize the use of commercially available handsets already in development for commercial cellular networks, and also to ensure maximum interoperability and roaming on commercial cellular networks.

Response: See the response to Comment #2 above.

Comment #5: A few commenters recommended that the application of this provision be performed in full conformance with the recommendation and guidelines on open, non-proprietary, commercially available standards found in the Section 4.1.8 of the Interoperability Board Report.

Response: FirstNet acknowledges the comment and believes its interpretations of 47 U.S.C. 1426(b)(2)(B) are consistent with the relevant Sections of the Interoperability Board Report.[13]

Comment #6: One commenter suggested that characterizing satellite connectivity as equipment ''for use on'' the network could result in requirements that constrict use of satellite connectivity as a network element, as opposed to an end-user device.

Response: FirstNet acknowledges the comment and will take the suggestion into consideration as it further delineates which specific equipment falls within the network components constituting the core network and RAN.

Comment #7: One commenter recommended that FirstNet should more clearly articulate what it means by ''connectivity'' so that interested parties can meaningfully evaluate whether the proposed scope of the requirement is reasonable and consistent with the Act's requirements.

Response: FirstNet, as stated in the *Second Notice,* interprets ''connectivity'' for the purposes of this provision as being satisfied by applying the requirements of 47 U.S.C. 1426(b)(2)(B) to only those parameters necessary to maintain interoperability and operational capability (*i.e.,* ''connectivity'') with the NPSBN as detailed in the Interoperability Board Report or otherwise in FirstNet network policies.

Comment #8: One commenter suggested that FirstNet, the National Institute of Standards and Technology (''NIST''), and the FCC should work to ensure that conformity with open, non-proprietary, commercially available standards—such as those developed by the 3rd Generation Partnership Project—is a prerequisite to appearing on the list of certified equipment that the Act instructs to be developed by NIST. The commenter also stated that NIST, FirstNet, and the FCC should work together to ensure rigorous interoperability verification when developing the list.

Response: FirstNet acknowledges the comment and intends to coordinate with NIST and the FCC as required by the Act.

Comment #9: Several commenters stated that the definition of equipment, or its interoperability requirements, should not preclude commercially developed and potentially legally protected materials, such as existing operating systems, from being acceptable platforms for accessing applications and connecting to the NPSBN, but rather, innovation and existing capabilities should be encouraged among the vendor community to reduce device costs and speed to deployment, so long as interoperability among various devices remains.

Response: FirstNet believes its interpretations do not preclude or hinder existing operating systems from being acceptable platforms for accessing applications and connecting to the NPSBN so long as these systems meet the relevant requirements of 47 U.S.C. 1426(b)(2)(B). Specifically, FirstNet concludes that the Act's goal of ''promot[ing] competition in the equipment market'' is satisfied by applying these requirements to only those parameters necessary to maintain interoperability (*i.e.,* ''connectivity'') with the NPSBN, which are included in the Interoperability Board Report or otherwise in FirstNet network policies. In reaching this conclusion, we recognized that in order for innovation to bring forth improved products for the NPSBN, and for FirstNet and public safety entities to benefit from competition, product differentiation must be allowed to thrive. However, such differentiation must be balanced with the interoperability goals of the Act. Thus, certain technical attributes of the network must be met by the equipment described pursuant to 47 U.S.C. 1426(b)(2)(B), but other equipment attributes may be left to individual vendors to develop.

Comment #10: One commenter stated that attributes and features of a particular product should, to the maximum extent possible, be traceable to a set of standard specifications.

Response: See the response to Comment #8 above.

B. FirstNet Network Policies

Network Policies

Under the Act, FirstNet is tasked with developing ''network policies'' in carrying out various obligations related to its mission to ensure the establishment of the NPSBN.[14] In particular, FirstNet must develop RFPs that appropriately address certain specified matters regarding building, operating, and maintaining the NPSBN, along with four other sets of policies covering technical and operational areas.[15] In addition to items related to the RFPs, FirstNet must develop policies regarding the technical and operational requirements of the network; practices, procedures, and standards for the management and operation of the network; terms of service for the use of the network, including billing practices; and ongoing compliance reviews and monitoring.[16] Taken as a whole, these policies, including the elements of the RFPs, form operating parameters for the NPSBN, addressing, for example, how the FirstNet core network will connect

[12] *Proposed Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012,* 79 FR 57058 (September 24, 2014) (herein ''*First Notice*'').

[13] *See* Interoperability Board, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network* (''Interoperability Board Report'') (May 22, 2012), *available at http://apps.fcc.gov/ecfs/document/view?id=7021919873.*

[14] *See* 47 U.S.C. 1426(c)(1).

[15] *See id.*

[16] 47 U.S.C. 1426(c)(1).

and operate with the RANs to ensure interoperability.

The Act does not expressly state whether only FirstNet, or both FirstNet and a State assuming RAN responsibilities, must follow the network policies required pursuant to 47 U.S.C. 1426(c)(1). Rather, the Act only refers to the ''nationwide public safety broadband network'' or the ''network,'' without expressly indicating whether such State RANs are included in the term. Thus, given the provisions of the Act, the Interoperability Board Report, the overall interoperability goals of the Act, and the effect on interoperability of not having the network policies apply to States assuming RAN responsibilities, FirstNet makes the following conclusions relating to the nature and application of the network policies developed pursuant to 47 U.S.C. 1426(c)(1) to both FirstNet and States assuming RAN responsibilities:

1. FirstNet concludes that the items listed in 47 U.S.C. 1426(c)(1)(A) relating to RFPs are ''policies'' for purposes of 47 U.S.C. 1426(c)(2) and as the term is generally used in 47 U.S.C. 1426(c).

2. FirstNet concludes that the network policies developed pursuant to 47 U.S.C. 1426(c)(1) apply to all elements of the network, including RANs deployed by individual States pursuant to 47 U.S.C. 1442(e)(3).

3. FirstNet concludes that a required aspect of a State's demonstrations of interoperability to both the FCC and NTIA under 47 U.S.C. 1442(e)(3), is a commitment to adhering to FirstNet's network policies implemented under 47 U.S.C. 1426(c).

4. FirstNet concludes that it could require compliance with network policies essential to the deployment and interoperable operation of the network for public safety in all States as a condition of entering into a spectrum capacity lease pursuant to 47 U.S.C. 1442(e)(3)(C)(iii)(II).

Analysis of and Responses to Comments on Network Policies

RFPs Items as Network Policies

Summary: The majority of commenters agreed with FirstNet's interpretation that the topics listed in 47 U.S.C. 1426(c)(1) pertaining to RFPs, while not typically thought of as policies, nonetheless are '' network policies'' for purposes of 47 U.S.C. 1426(c)(1).

Comment #11: One commenter disagreed that the RFP-related items *should* be considered policies, but acknowledged that they would qualify as such pursuant to the Act as written.

Response: FirstNet acknowledges the comment, but believes its interpretation of this provision as recognized by the commenter, is correct pursuant to the Act.

Applicability of Network Policies to States Assuming RAN Responsibilities

Summary: The vast majority of commenters also agreed with FirstNet's interpretation that the network policies pursuant to 47 U.S.C. 1426(c) apply regardless of whether FirstNet deploys the RAN or the State takes on that responsibility. These commenters agreed with FirstNet's assessment that universal application of network policies, irrespective of who deploys the RAN, is critical to maintaining interoperability throughout the NPSBN.

Comment #12: A few commenters disagreed with FirstNet's interpretation that all States must comply with FirstNet's network policies, generally arguing that States assuming responsibilities for deploying the RAN are not compelled pursuant to the Act to comply with FirstNet's network policies and thus should have the authority to develop their own policies.

Response: FirstNet disagrees and believes the network policies required to be developed pursuant to 47 U.S.C. 1426(c)(1) to be applicable to the entire NPSBN, including a RAN whether such RAN is deployed by FirstNet or a State.

First, the plain language of the Act suggests that network policies developed pursuant to 47 U.S.C. 1426(c)(1) are intended to apply to all elements of the NPSBN. The Act defines the term ''nationwide public safety broadband network'' to mean the nationwide, interoperable public safety network described in 47 U.S.C. 1422.[17] Accordingly, the Act, in 47 U.S.C. 1422(b), expressly defines the NPSBN as initially consisting of two primary components: The core network and the RAN. Although generally describing the elements and scope of these network components, the Act does not exclude or otherwise indicate that a State-deployed RAN is not part of the NPSBN. Thus, the plain language of the Act appears to indicate that a RAN, regardless of what entity actually deploys it, is a component of the overall NPSBN. Consequently, it is reasonable to interpret that a RAN, as a component of the network, would be subject to all network requirements, regardless of what entity is responsible for deploying the RAN, including policies that apply to the network as a whole.

Second, the Act mandates that FirstNet, in carrying out the requirements of the Act, must establish *network* policies, but does not authorize any other entity to establish such policies.[18] Specifically, FirstNet must develop the following policies: Those related to technical and operational requirements of the *network;* practices, procedures, and standards for the management and operation of such *network;* terms of service for the use of such *network,* including billing practices; and ongoing compliance reviews and monitoring of the management and operation of the *network* and practices and procedures of entities operating on the *network* and the personnel using the *network.*[19] This list of network policies described in 47 U.S.C. 1426(c)(1) does not expressly contemplate that a separate set of network policies would be developed or apply to a RAN deployed by a State. In fact, the Act, by requiring FirstNet to consult with States on various matters, including network policies, suggests that the opposite conclusion is likely the case. For example, as stated in the *Second Notice,* the Act did not differentiate between States accepting the FirstNet RAN plan and States assuming RAN responsibility in the provisions of 47 U.S.C. 1426(c)(2) requiring consultation with States on the network policies of 47 U.S.C. 1426(c)(1). Consequently, such consultations presumably would not be required for States assuming RAN responsibility if the policies in question did not apply to the RAN in that State.

Third, among other network considerations, the Act describes the process a State seeking to conduct it own RAN deployment must follow in order to receive approval of an alternative RAN plan, a grant for RAN construction, and authority to seek a spectrum capacity lease with FirstNet. These considerations include, among other things, a demonstration of initial and ongoing interoperability with the NPSBN.[20] From a practical perspective, such interoperability will largely depend, as is the case with FirstNet's deployed core network and RANs, on compliance with the network policies developed pursuant to 47 U.S.C. 1426(c)(1). Thus, a necessary aspect of a State's demonstration of interoperability to both the FCC and NTIA is a commitment to adhering to FirstNet's network policies. This could be particularly important because such policies will likely evolve over time as the technology, capabilities, and operations of the network evolve, and

[17] 47 U.S.C. 1401(21).

[18] *See* 47 U.S.C. 1426(c)(1).

[19] *See id.*

[20] 47 U.S.C. 1422(e)(3).

an alternative interpretation could frustrate the interoperability goals of the Act.

In addition, States assuming RAN responsibilities must demonstrate ''comparable security, coverage, and quality of service to that of the [NPSBN].'' [21] FirstNet's policies will establish requirements for security, coverage, and quality of service standards for the NPSBN, and thus States seeking to assume State RAN responsibilities would need to demonstrate ''comparable'' capabilities to those specified in these policies. As stated above, however, the Act requires FirstNet to engage in consultation with States regarding the network policies pursuant to 47 U.S.C. 1426(c)(1), so while FirstNet will establish such policies, States will have meaningful opportunities to help inform the establishment of such policies.

Comment #13: A few commenters recognized the importance of interoperability, but suggested that States taking on RAN responsibilities should have the flexibility to tailor their policies to their unique circumstances unless it affected interoperability.

Response: FirstNet understands the unique needs of the States and believes the Act, through its extensive consultation requirements and processes regarding network policies developed pursuant to 47 U.S.C. 1426(c)(1), provides a vehicle for States to have substantial opportunities to inform such policies and, as is discussed in the *Second Notice,* FirstNet will continue to work cooperatively with States in their establishment.

Comment #14: One commenter advocated that, in order to avoid imposing unnecessary burdens, States assuming RAN responsibilities should be required to comply with only those policies necessary to maintain interoperability.

Response: FirstNet agrees that the primary goal of the Act is to ensure the interoperability of the NPSBN, and, accordingly, paramount among network policies are those that assist in meeting this requirement. However, the Act requires FirstNet to establish policies for other elements critical to establishing the NPSBN, such as those that govern the technical and operational requirements of the network.[22] For example, such policies, as contemplated in the Act, will likely provide the criteria and processes for the implementation and monitoring of vital network features, including those related to priority and preemption or network security, both of which are essential to public safety. To that end, it is critical that public safety be afforded the same features, functionality, and level of service from State to State, particularly when there is a need to cross State boundaries in the case of an incident, to ensure no impact to vital communications. The Act's requirement pursuant to 47 U.S.C. 1426(c)(1) for the implementation of network policies, we believe, was reasonably intended to apply to States assuming RAN responsibilities to ensure neither the public's safety nor the network are put at risk. Accordingly, FirstNet disagrees that States assuming RAN responsibilities should be required to comply with only those network policies necessary to maintain interoperability.

Compliance With FirstNet Network Policies as an Element To Demonstrating Interoperability

Summary: A majority of commenters agreed with FirstNet's related interpretation that adherence to FirstNet's network policies would be an important factor in demonstrating interoperability pursuant to 47 U.S.C. 1442(e)(3) by a State that is seeking to assume RAN responsibilities. Several of these commenters focused on the need for uniformity and consistency in policies to ensure interoperability throughout the lifetime of the network. A few commenters disagreed with this approach, however, suggesting that the interpretation was not supported by the Act.

Comment #15: One commenter contended that the Act neither expressly nor implicitly makes such a pronouncement regarding a State's interoperability demonstration, expressed concern that the interpretation could compromise a State's ability to have control over deployment of its RAN, and proposed instead that a State seeking to assume responsibility for deploying the RAN be required to demonstrate both current and future interoperability capability, but not necessarily be subject to FirstNet's network policies.

Response: See the responses to Comment #1 and Comment #2 above.

Compliance With FirstNet Network Policies as a Condition To Obtaining a Spectrum Capacity Lease

Summary: Commenters largely agreed with FirstNet's conclusion that it could require compliance with certain network policies essential to the deployment and interoperable operation of the NPSBN as a condition to entering into a spectrum capacity lease pursuant to 47 U.S.C. 1442(e)(3)(C)(iii)(II). One commenter, for instance, encouraged FirstNet to use all the tools at its disposal to require compliance with network policies to ensure the central goal of the Act of creating a sustainable, interoperable, nationwide network. Another commenter noted that, as the license holder of the spectrum, FirstNet has the right to take measures that ensure the nationwide interoperability of the network. A few commenters disagreed with FirstNet's interpretation that compliance with FirstNet's network policies could be a condition within a State's eventual spectrum capacity lease with FirstNet, challenging FirstNet's authority pursuant to the Act to impose such a condition.

Comment #16: One commenter argued that the only limitations allowed to be placed on access to a spectrum capacity lease are those expressly enumerated in 47 U.S.C. 1442(e)(3)(D), indicating that compliance with FirstNet's network policies are not explicitly included in those requirements.

Response: FirstNet disagrees and notes that as the licensee of the spectrum it must ultimately determine the terms and conditions of a spectrum capacity lease entered into with a State assuming responsibility for RAN deployment.

Comment #17: One commenter contended that requiring compliance with network policies as a condition to obtaining a spectrum capacity lease was a way for FirstNet to gain concessions not required pursuant to the Act from a State seeking to take on responsibilities for deploying the RAN.

Response: FirstNet recognizes the Act strikes a balance between establishing a nationwide network and providing States an opportunity, under certain conditions, to deploy a RAN within their respective State boundaries. One of those conditions explicitly stated within the Act is for the State to obtain a spectrum capacity lease from FirstNet.[23] Accordingly, FirstNet intends to act in good faith with each of the States to explore ''win-win'' solutions with States desiring to assume RAN responsibilities consistent with all requirements in the Act mandating the deployment of an interoperable nationwide broadband network for public safety.

Comment #18: A few commenters did not disagree with FirstNet's interpretation, but noted the importance of providing clarity and transparency to the spectrum capacity leasing process.

Response: FirstNet acknowledges the comments and will consider them, as appropriate, in the development of any

[21] 47 U.S.C. 1442(e)(3)(D)(iii).

[22] *See* 47 U.S.C. 1426(c)(1).

[23] *See* 47 U.S.C. 1442(e)(3)(C)(iii)(II).

processes or requirements related to a spectrum capacity lease.

C. A State's Opportunity To Assume Responsibility for RAN Deployment and Operations

Final Interpretations Regarding the Presentation of a State Plan and the Completion of Request for Proposal Process

The Act requires FirstNet to present its plan for a State to the Governor ''[u]pon the completion of the request for proposal process conducted by FirstNet for the construction, operation, maintenance, and improvement of the [NPSBN] . . . .'' [24] The Act does not further define the specific stage in the RFP process that would constitute being ''complete.''

FirstNet, in accordance with its analysis in the *Second Notice,* makes the following conclusions regarding the completion of the RFP process and the definition of completion:

1. FirstNet interprets 47 U.S.C. 1442(e) to merely require completion of the RFP process for a particular State, rather than the nation as a whole, prior to presentation of the plan to such State, assuming that FirstNet can at that stage otherwise meet the requirements for presenting a plan (and its contents) to such State.

2. FirstNet concludes that ''completion'' of the RFP process occurs at such time that FirstNet has obtained sufficient information to present the State plan with the details required pursuant to the Act for such plan, but not necessarily at any final award stage of such a process.

Analysis of and Responses to Comments on the Completion of the Request for Proposal Process

The majority of respondents agreed with FirstNet's interpretation that, so long as FirstNet is able to provide the contents of, and meet the Act's requirements for presenting, a plan to the State, FirstNet need only complete the RFP process for the specific State rather than the nation as a whole.[25] In addition, most commenters agreed that ''completion'' was not necessarily a final award stage of any RFP process, but simply the stage at which FirstNet has obtained sufficient information to present the State plan and its required details to the Governor. Commenters generally understood the complex economies of scale determinations that must be undertaken by potential offerors and agreed that, depending on final determinations by the States regarding their decision to assume responsibility to deploy their own RAN, such final award stages may come after the State plan presentation.

Several respondents disagreed, however, arguing that the RFP process must be completed nationwide prior to any State plan being presented to the Governor or his designee, while other commenters provided recommendations for implementing these interpretations.

Comment #19: Two commenters were concerned that FirstNet intended to issue individual RFPs for each State, and that such an approach would deprive FirstNet and NTIA of critical information and prevent States from making informed decisions. One commenter stated that whether FirstNet chooses to conduct a single nationwide RFP for the entire network, discrete nationwide RFPs for categories of network procurements, or multiple State or regional RFPs, FirstNet should complete all of its planned RFP processes across the nation before presenting individualized State plans.

Response: FirstNet disagrees that all RFP processes across the nation must be completed prior to presenting a single State plan, and believes that requiring such a process would have the potential to restrict the number and kind of RFPs that FirstNet issues, and could unduly delay the deployment of the NPSBN to the injury of public safety stakeholders and potential partner(s).

The Act provides FirstNet with flexibility in deciding how many and what type of RFPs to develop and issue by not specifying any such required number or type.[26] As discussed in the *Second Notice,* if 47 U.S.C. 1426 is read to require all States to await the completion of all such RFP processes, FirstNet would likely constrain the range of RFPs it might otherwise conduct to avoid substantial delays nationwide, and in doing so constrain its ability to reflect the input from consultative parties as required by the Act.[27]

Additionally, by requiring FirstNet to wait until all RFP processes are fully complete across the nation prior to issuing a State plan, a single protest regarding a single State or region could substantially delay implementation of the network in many or most States contrary to the Act's emphasis on ''speed[ing] deployment of the network.'' [28]

Comment #20: Another commenter focused on the potential for diminished spectrum value were FirstNet to issue individual State RFPs and was particularly concerned that there may be a lack of respondents to the RFPs in rural States with less overall spectrum value than those States that have larger, metropolitan areas within their respective borders. This commenter asserted that the only way to meet the Act's requirements to ''build out the NPSBN to cover rural America'' was to either partner with a large number of rural providers or to have a nationwide partner.

Response: FirstNet acknowledges the comment and will consider it, as appropriate, in the development of any processes or requirements related to RFP(s) regarding the build out of the NPSBN.

Comment #21: An additional commenter was concerned that if complete nationwide data from the RFP process is not available to a State when FirstNet presents the State plan, any alternative plan developed by the State could not be fairly evaluated for its '' 'cost-effectiveness' based on a nationwide analysis.''

Response: FirstNet disagrees that full nationwide data is necessary for a State to develop an alternative plan. FirstNet interprets that, in order to present a State plan, FirstNet must have obtained sufficient information to present the State plan with the details required pursuant to the Act for such a plan. The details of the State plan, as discussed in the *Second Notice,* must include sufficient information to enable NTIA to undertake comparisons of cost-effectiveness, security, coverage, and quality of service—exactly the type of cost-effectiveness comparisons about which the commenter is concerned. Therefore, FirstNet believes its final interpretation regarding what constitutes completion of the RFP process necessarily encapsulates and allays the commenter's concerns.

Comment #22: Several commenters, while agreeing with FirstNet's legal interpretations that the RFP process is considered complete when FirstNet has enough information to present a State plan for the specific State in question, also suggested that FirstNet try to at least provide State plans at a similar time to members of the surrounding FEMA region due to the close coordination that must take place within FEMA region States.

Response: FirstNet acknowledges this comment and will consider it, as appropriate, as it develops the process for the presentation of State plans.

[24] 47 U.S.C. 1442(e).

[25] We note that that the FCC may provide further guidance with respect to the approval process for an alternative plan pursuant to 47 U.S.C. 1242(e)(3).

[26] *See generally* 47 U.S.C. 1426(b).

[27] *See* 47 U.S.C. 1426(c)(2)(A).

[28] *See* 47 U.S.C. 1426(b)(1)(C).

Final Interpretations Regarding the Content of a State Plan

47 U.S.C. 1442(e)(1) requires that FirstNet provide to the Governor of each State, or a Governor's designee, ''details of the proposed plan for build out of the [NPSBN] in such State.'' Section 1442 does not include any express guidance as to the ''details of the proposed plan'' that must be provided.

Other provisions of the Act, however, provide some guidance in this regard and include provisions relating to the outcomes of the RFP process as well as the ability for NTIA to make comparisons of cost-effectiveness, security, coverage, and quality of service. In accordance with the structure and purposes of the Act, FirstNet makes the following interpretations regarding the content of a State plan:

1. FirstNet concludes that the details of the proposed State plan pursuant to 47 U.S.C. 1442(e)(1)(B) should include at least certain outcomes of the RFP process.

2. FirstNet concludes that the FirstNet plan must contain sufficient information to enable NTIA to make comparisons of cost-effectiveness, security, coverage, and quality of service.

Analysis of and Responses to Comments on the Content of a State Plan

The majority of commenters agreed with FirstNet's interpretations regarding the content of a State plan. Many agreed with FirstNet that its interpretations regarding the content of a State plan constituted only the minimum details that FirstNet should provide and that FirstNet may decide to provide more specifics as it deems necessary. A few commenters, while generally agreeing with FirstNet's conclusions, suggested additional details that FirstNet should take into consideration and provide upon the presentation of a State plan.

Comment #23: One commenter suggested that any State plan must also contain information and assumptions regarding the core network, including capacity, accessibility, and interoperability, for a Governor to truly have enough information at hand to make an informed decision.

Response: FirstNet agrees that certain information, as determined by FirstNet, regarding the core network should be included in the State plan in order to enable the FCC and NTIA to effectively evaluate and compare the State's alternative RAN plan should the State decide to deploy its own RAN and not participate in the FirstNet-proposed State plan pursuant to 47 U.S.C. 1442(e)(2).

Comment #24: Several commenters stated that any and all information, data, and analysis that FirstNet uses to develop the State plan must be fully and completely available for a State to completely understand all decisions that went into the State plan and make an informed decision.

Response: FirstNet disagrees and notes that the Act does not require that such information be provided in a State plan.[29]

Governor's Role in the State Plan Process

47 U.S.C. 1442(e)(2), entitled ''State decision,'' establishes the Governor's role in choosing how the State will proceed regarding FirstNet deployment. FirstNet makes the following interpretations regarding the Governor's role in the State plan process and the ability of FirstNet and the States to implement additional State RAN deployment:

1. FirstNet concludes that the decision of the Governor pursuant to 47 U.S.C. 1442(e)(2), for purposes of the Act, is binding on all jurisdictions within such State, and that such a decision must be made for the entire State in question and not simply a subset of individual jurisdictions.

2. FirstNet concludes that FirstNet and a State could agree that FirstNet and the State (or sub-State jurisdictions) work together to permit implementation of added RAN coverage, capacity, or other network components beyond the State plan to the extent the interoperability, quality of service, and other goals of the Act are met.

Analysis of and Responses to Comments on the Governor's Role in the State Plan Process

Summary: The majority of commenters agreed that the Act specifies the Governor as the State official who makes a final determination regarding FirstNet deployment in the State and agreed that the Governor's decision should be binding on all jurisdictions within the State. Commenters also generally agreed with FirstNet's interpretation that FirstNet and States could work together to potentially expand RAN coverage, capacity, or other network components so long as the goals of the Act were met. A few commenters, as described below, expressed some general concerns about a Governor's authority to make a decision related to RAN deployment within the State.

Comment #25: Several commenters detailed, while agreeing with FirstNet's interpretation that the ultimate decision regarding FirstNet deployment in the State was that of the Governor, that many States may require legislative approval or coordination between political subdivisions or counties and the State before the Governor is able to make such decisions for the State.

Response: FirstNet acknowledges the comment and believes regardless of whether a Governor may need to seek certain approvals prior to making a decision for the State, pursuant to the Act, the final State decision regarding a FirstNet-proposed State plan continues to ultimately rest with the Governor.[30]

Comment #26: One commenter suggested that plans for each State should be developed after appropriate consultation with tribal jurisdictions in order for the plan to be binding on tribal jurisdictions. The commenter stated that in the event of a tribal/State dispute, approval for the State plan should not be delayed for the rest of the State and coverage or level of service for the tribal jurisdiction could be ''amended to the FirstNet or Commission approved plan.''

Response: Tribal jurisdictions are expressly included as part of the statutorily mandated consultation process.[31] The Act specifies that such consultation regarding the development of State plans must occur between FirstNet and the State single point of contact (''SPOC'').[32] FirstNet has endeavored, and will continue, to seek input in accordance with the Act from tribal jurisdictions in an effort to ensure that their needs are reflected in the State plan ultimately delivered to a Governor. While it is not entirely clear what the commenter means by having tribal coverage levels be ''amended to the FirstNet or Commission approved plan,'' FirstNet does agree that there may be opportunities for the State and FirstNet to agree to have FirstNet and the tribal jurisdictions work directly with one another to provide added RAN coverage, capacity, or other network components as necessary beyond the State plan so long as the interoperability, quality of service, and other goals of the Act are met.

Comment #27: One commenter stated that FirstNet wrongly concludes that a Governor's decision would prevent a city or county within the State from deploying its own RAN. The commenter asserts that if a jurisdiction chooses to fund and build its own RAN, it should be allowed to do so and mentions that, regardless, ''the jurisdiction would be within its rights to seek licensure and

[29] *See* 47 U.S.C. 1442(e)(1).

[30] *See* 47 U.S.C. 1442(e)(2).

[31] *See* 47 U.S.C. 1426(c)(2).

[32] *See id.*

operate a network within its jurisdiction.''

Response: FirstNet disagrees with the commenter's assertions. 47 U.S.C. 1442(e)(2) clearly states that ''the Governor shall choose whether to participate in the deployment of the [NPSBN] as proposed by [FirstNet] or conduct its own deployment of a [RAN] in such State.'' [33] As discussed in the *Second Notice,* such sub-State level decisions, if permitted, could create potential islands of RANs which do not meet the interoperability and other goals of the Act regarding a NSPBN.[34] The Act does not authorize anyone other than the Governor to make a respective State's decision regarding the FirstNet-proposed State plan and, in fact, further supports the conclusion of a single decision point through the creation of a single point of contact for each State, directly appointed by the Governor.[35]

In addition, the Act grants FirstNet the nationwide license for the 700 MHz D block spectrum and existing public safety broadband spectrum [36] and requires a ''State'' (not individual sub-State jurisdictions) that seeks to assume RAN responsibilities to ''submit an alternative plan'' to the FCC and apply to NTIA to lease spectrum capacity from FirstNet.[37] Nowhere does the Act contemplate sub-State jurisdictions operating their own RANs using FirstNet's licensed spectrum—it is only a State that may develop an alternative plan for submission through the section 1442(e)(3)(C) approval process for eventual negotiation of a spectrum capacity lease with FirstNet.

Comment #28: One commenter suggested that, while agreeing with FirstNet's conclusion that it could work with the State to permit State or sub-State implementation of added RAN coverage, capacity, or other network components beyond the FirstNet plan, FirstNet should not enter any agreement on a Statewide or sub-State basis without the concurrence of the State, or otherwise in a manner that would limit or restrict the Governor's discretion and rights with regard to the State decision process pursuant to the Act.

Response: FirstNet agrees with this comment and, as indicated in the *Second Notice,* would work with the State prior to any such agreements.

[33] 47 U.S.C. 1442(e)(2)(1).

[34] *See* 47 U.S.C. 1422(a).

[35] *See* 47 U.S.C. 1442(d).

[36] *See* 47 U.S.C. 1421(a).

[37] *See* 47 U.S.C. 1442(e)(3).

Final Interpretations Regarding the Timing and Nature of a State's Decision

The Act provides that the Governor must make a decision ''[n]ot later than 90 days after the date on which the Governor of a State receives notice pursuant to [section 1442(e)(1)].'' [38] As noted in the *Second Notice,* such phraseology raises the question as to whether a Governor could make such a decision prior to receiving the notice contemplated pursuant to section 1442(e)(1). Additionally, if the Governor decides to participate in the State plan, the Act does not specifically require the Governor to provide notice of the State's decision to participate in the FirstNet-proposed network to FirstNet, or any other parties.[39]

Finally, if the Governor decides to assume RAN responsibilities on behalf of the State and create an alternative plan for deployment of the RAN within its borders, the Act provides that ''[u]pon making a decision . . . the Governor shall notify [FirstNet], the NTIA, and the [FCC] of such decision.'' [40]

After taking into consideration the analysis contained in the *Second Notice* and its associated comments, FirstNet makes the following interpretations regarding the timing and nature of a State's decision:

1. FirstNet concludes that the Governor must await notice and presentation of the FirstNet plan prior to making the decision pursuant to 47 U.S.C. 1442(e)(2).

2. FirstNet concludes that a State decision to participate in the FirstNet-proposed deployment of the network in such State may be manifested by a State providing either (1) actual notice in writing to FirstNet within the 90-day decision period or (2) no notice within the 90-day period established pursuant to 47 U.S.C. 1442(e)(2).

3. FirstNet interprets the requirement within 47 U.S.C. 1442(e)(3) stating that the notice is to be provided to FirstNet, NTIA, and the FCC as being an immediate (*i.e.,* same day) requirement.

Analysis of and Responses to Comments Regarding the Timing and Nature of a State's Decision

The majority of commenters agreed with FirstNet's interpretations regarding the timing and nature of a State's decision. Several commenters affirmed that the Act requires certain findings and comparisons to be made during the process under which a State assumes RAN responsibility and that such a comparison cannot be conducted until the FirstNet plan has been presented.

Some commenters, however, disagreed with FirstNet, stating that a Governor is free to make a decision at any time and should be allowed to make the decision to assume responsibility for the RAN early if the State so chooses, as well as be allowed the full 90 days to inform FirstNet, NTIA, and the FCC of the State's decision regardless of when a decision is actually made within a State. Additionally, some commenters asked that the Governor be allowed time beyond the 90-day limit to make such a decision. Others, while agreeing with FirstNet's legal conclusions, suggested that FirstNet try to provide the States with as much information as possible prior to the official 90-day clock to assist the Governors with their decision. Finally, some commenters disagreed with FirstNet's conclusion that only an affirmative opt-out notice would result in a State not accepting the State plan presented by FirstNet.

Comment #29: Several commenters stated that FirstNet has no authority to instruct a Governor on his or her decision-making process. These commenters stated that FirstNet should not become an obstacle requiring States to wait to make a decision to assume RAN responsibility.

Response: To clarify, FirstNet acknowledges that it has no authority to instruct a Governor on his or her specific decision-making process, but rather only to interpret the requirements with respect to the process for submitting that ultimate decision as provided in the Act.

The Act provides that ''[n]ot later than 90 days *after the date on which the Governor of a State receives notice* pursuant to [section 1442(e)(1)], the Governor shall choose whether to (A) participate in the deployment of the [NPSBN] as proposed by [FirstNet] or (B) conduct its own deployment of a [RAN] in such State.'' [41] While many commenters seemed to focus on the ''*not later than 90 days*'' phrase at the beginning of the sentence and assert this to mean that a Governor may choose to assume RAN responsibility at any time between the present day up to the 90-day time limit, the decision is expressly dependent on FirstNet having first provided the Governor the requisite notice pursuant to section 1442(e)(2).

For instance, it is logical to conclude that a Governor could wait the full 90 days after he or she receives notice of the State plan before making the decision to assume RAN responsibility and notify the proper parties. Similarly,

[38] *See* 47 U.S.C. 1442(e)(1).

[39] *See* 47 U.S.C. 1442(e)(3)(A).

[40] *Id.*

[41] 47 U.S.C. 1442(e)(2) (emphasis added).

a Governor could wait, for example, only 40 days after he or she receives notice, or even make the decision required pursuant to section 1442(e)(2) and notify the proper parties the same day as receiving notice of the State plan. By using the language ''after the date on which the Governor of a State receives notice,'' Congress indicated its intent that the State decision would occur *after* receipt of the notice from FirstNet. Thus, for purposes of the formal State decision pursuant to section 1442(e)(2), the Governor must wait until the FirstNet-proposed State plan is presented before he or she notifies FirstNet, NTIA, and the FCC of the State's decision to assume RAN responsibility.

Furthermore, it would be counterproductive to notify FirstNet, NTIA, and the FCC of the State's decision earlier than presentation by FirstNet of the State plan as that would necessarily start the 180-day clock regarding submission of an alternative plan without there being any FirstNet proposed plan against which the FCC and NTIA could evaluate and compare the State's alternative plan.[42] As such, these entities would be unable to fulfill their statutory responsibilities related to approving or rejecting the alternative plan as they would have insufficient information to make the necessary determinations as required under the Act.

Comment #30: Some commenters suggested that FirstNet should work with States where there are opportunities for early deployment and allow the State to amend their alternative plans at a later stage in the process as needed once the State plan is presented by FirstNet, the goal of which would be to allow the States to move forward with deployment as soon as the State was ready.

Response: The Act explicitly requires a sequential process to be followed prior to any FirstNet network deployment taking place.[43] It is not until the State has decided to participate in FirstNet's proposed State plan or has progressed through the entire alternative plan process provided in section 1442(e)(3) that any network deployment may begin. To proceed through the process required under section 1442(e)(3)(C)-(D), the FCC and NTIA must have access to the FirstNet-proposed State plan in order to compare it to the State's alternative plan.[44]

The Act does not contemplate any type of retroactive amendment process within section 1442(e)(3) and requires comparisons and evaluations to take place between the FirstNet-proposed State plan and the State's alternative plan that simply cannot occur without the FirstNet proposed State plan first being presented to the Governor as required by the Act. Without a FirstNet plan having been presented, the State's premature decision would not enable the FCC to make the assessments required to approve the State's alternate plan, or if such plan is approved, enable NTIA to review and determine whether to approve an application for grant funds and to seek a spectrum capacity lease from FirstNet.

Comment #31: One commenter stated that FirstNet should make clear that Governors are not prohibited from beginning to develop alternative plans now and that the development of alternative plans in advance could also assist Governors in making informed choices regarding whether to assume RAN responsibility or participate in the FirstNet State plan.

Response: There is no statutory provision preventing States from using their own funds to begin developing alternative plans.

Comment #32: A few commenters asserted that the State must respond in writing with its decision, regardless of the 90-day time limit prior to FirstNet taking any action.

Response: As stated in the *Second Notice,* the Act does not require the Governor of a State to provide notice of the State's decision to participate in FirstNet's proposed State plan pursuant to section 1442(e)(2)(A) to FirstNet, or any other parties. Rather, notice is only required should the Governor of a State decide that the State will assume responsibility for the buildout and operation of the RAN in the State.[45]

Taking into consideration the Act's emphasis on the need ''to speed deployment'' of the network for public safety,[46] the requirement for specific required affirmative notice for a decision to assume RAN deployment and operation, and no such explicit affirmative notice required for a decision to accept the proposed FirstNet plan, FirstNet concludes that notice is not required within the 90-day period established pursuant to section 1442(e)(2) in order for a Governor to choose to participate in the FirstNet-proposed State plan.

Comment #33: Several commenters asked that States be given longer than the 90-day time limit established by the Act due to the complexity of the decision itself and the decision process that many Governors may have to go through prior to making a final determination regarding whether to choose to participate in the FirstNet-proposed State plan or conduct the deployment of the State's own RAN. In addition, some commenters expressed frustration that FirstNet will have several years to decide its approach with the States, whereas the States must provide written notice of its intentions within 90 days.

Response: FirstNet was created by Congress and is bound by the statutory language contained within the Act. The Act explicitly provides for a 90-day period following the presentation of the State plan for a Governor to choose to participate in the State plan as presented by FirstNet or choose to conduct its own deployment of a RAN within the State.[47] FirstNet has no ability to change the plain language of the Act and therefore has no authority to extend the 90-day time period.

Comment #34: Some commenters suggested that, while FirstNet is unable to provide the Governor with more time following the presentation of the FirstNet-proposed State plan, FirstNet should do everything in its power to provide the States with information that may be contained in the State plan as much in advance of the formal 90-day time clock as possible.

Response: FirstNet acknowledges the comment and plans to continue to coordinate with the States through its ongoing consultation efforts to share details of the proposed State plans as such information comes available as part of the RFP process.

The Nature of FirstNet's Proposed State Plan

The Act pursuant to 47 U.S.C. 1442(e)(1) requires FirstNet to present a ''plan'' to the Governor, or to the Governor's designee, of each State. The Governor then must decide whether to participate in the deployment as proposed by FirstNet or to deploy the State's own RAN that interoperates with the NPSBN.[48] While the presentation of such a plan is an important step in the deployment of the NPSBN, it is only one additional milestone within the ongoing relationship between FirstNet and the States, with significant collaboration between the parties still to take place prior to deployment.

Using the plain language of the Act, a ''plan,'' as defined by Oxford

[42] *See* 47 U.S.C. 1442(e)(3)(C)–(D).

[43] *See* 47 U.S.C. 1442(e).

[44] *See* 47 U.S.C. 1442(e)(3)(C)–(D).

[45] *See* 47 U.S.C. 1442(e)(3)(A).

[46] *See, e.g.,* 47 U.S.C. 1426(b)(1)(C); *see also, e.g.,* 47 U.S.C. 1426(b)(3).

[47] *See* 47 U.S.C. 1442(e)(2).

[48] *See* 47 U.S.C. 1442(e)(1)(B).

Dictionaries, is a ''detailed proposal for doing or achieving something.'' [49]

Nowhere does the Act use contract terminology, such as ''offer,'' ''execute,'' or ''acceptance,'' in relationship to the FirstNet plan. In fact, the Act speaks only to a Governor's decision to ''participate'' in the deployment as proposed by FirstNet.[50] Accordingly, FirstNet makes the following conclusion regarding the nature of FirstNet's proposed State plan:

FirstNet concludes that the presentation of a plan to a Governor and his/her decision to either participate in FirstNet's deployment or follow the necessary steps to build a State RAN do not create a contractual relationship between FirstNet and the State.

Analysis of and Responses to Comments Regarding the Nature of FirstNet's Proposed State Plan

The majority of commenters agreed with FirstNet's conclusion that the presentation of the State plan and the Governor's decision to (or not to) participate in the plan do not constitute a contractual relationship between the parties. Several commenters expressed their sentiments that any network user fees associated with the network could not be binding on individual public safety entities at the time of the State plan because not all such fees will likely be known at the time a State plan is presented by FirstNet, and therefore a contract could not exist between the parties. Moreover, the vast majority of respondents agreed that it would not be until public safety entities actually subscribe to the NPSBN that contractual relationships would be established between the public safety entities themselves and FirstNet or the State, as applicable.

Comment #35: Several commenters, while agreeing with FirstNet's interpretation that the plan does not constitute a contract, stated that any material alteration of the State plan by FirstNet, such as priority or timing of build-out, should also allow a State to similarly alter its decision that was based on the previous plan.

Response: The Act does not provide for any mechanism whereby a Governor that decides to participate in the FirstNet-proposed State plan pursuant to 47 U.S.C. 1442(e)(2) can then reverse his or her decision for the State and choose to assume RAN responsibility at some unspecified point in the future. Once a Governor is presented with the FirstNet-proposed State plan, he or she then has 90 days with which to make the decision to participate in FirstNet's proposed plan or to choose to conduct its own State RAN deployment.[51] Congress struck a balance in the Act between a State's right to conduct its own RAN deployment and FirstNet and its potential partner(s)' needs for certainty as network deployment begins nationwide. Both FirstNet and its ultimate network partner(s) must be able to rely on State decisions in order to effectively and efficiently plan the nationwide deployment of the NPSBN.

FirstNet recognizes that after a Governor's decision, changes to the FirstNet State plan could arguably occur due to unforeseen circumstances or even based on further agreements between FirstNet and the impacted State. FirstNet intends to continue to coordinate closely with each State as it plans the deployment in accordance with the State plan to help ensure such plans meet the needs of public safety. It is important to note that as there is no mandate in the Act that public safety purchase services from FirstNet, FirstNet must offer an attractive value proposition to incentivize adoption of the NPSBN by its public safety stakeholders.

Comment #36: One commenter expressed that the Act, specifically 47 U.S.C. 1442(e)(3)(C)–(D), requires that the State demonstrate specific criteria in its alternative plan in order to be approved by the FCC and NTIA and to enter a spectrum capacity lease with FirstNet. Therefore, while the commenter agrees that the FirstNet-proposed State plan does not constitute a contract between the State and FirstNet, the commenter believes that the State should expect certainty regarding these specific criteria for an alternative plan. Without such a guarantee, the commenter asserts that States will not be provided with the information needed to make an appropriate RAN deployment decision.

Response: FirstNet, as discussed in the *Second Notice,* intends to include at least certain outcomes of the RFP process as well as sufficient information to enable NTIA to make comparisons of cost-effectiveness, security, coverage, and quality of service.

Comment #38: Several commenters disagreed that FirstNet's State plan does not form a contract between FirstNet and the State. A few commenters argued that FirstNet's presentation of a State plan to a State constituted an ''offer'' to the Governor, with ''acceptance'' of such offer occurring when the Governor chooses to participate in the offered plan. One commenter suggested that FirstNet's State plan in essence creates an ''unconscionable contract of adhesion'' by not containing what the commenter considered to be ''material elements of the contract.'' Furthermore, these commenters contended that without the State plan presentation and acceptance being considered a binding contact, the State cannot obtain the necessary certainty with which to make an informed decision pursuant to 47 U.S.C. 1442(e)(2).

Response: FirstNet disagrees with this comment and concludes, as discussed in the *Second Notice,* that the presentation of a proposed plan to a State from FirstNet does not create any type of contract. First, the applicable provisions of the Act do not use, nor make any reference to, any contract terminology in describing the State plan, thus suggesting that Congress did not intend for such plans to create a contract between FirstNet and the States. Next, as analyzed in the *Second Notice,* the presentation of the State plan does not constitute the necessary elements of ''offer and acceptance'' to create a contract. Finally, unlike the plan itself that does not mandate any entity subscribe to any eventual FirstNet service offering, if public safety entities ultimately decide to purchase FirstNet services, at that time a contract will be established between the parties with the typical terms and conditions of a contractual relationship.

Final Interpretations Regarding the State's Development of an Alternative Plan

47 U.S.C. 1442(e)(3)(B) requires, not later than 180 days after a Governor provides notice to FirstNet, NTIA, and the FCC pursuant to 47 U.S.C. 1442(e)(3)(A), that the Governor develop and complete RFPs for construction, maintenance, and operation of the RAN within the State. Similar to the requirement that FirstNet must notify the State upon the ''completion'' of the RFP process,[52] section 1442(e)(3)(B) does not further define the phrase ''complete requests for proposals'' that the State must accomplish within the 180-day timeline.

As stated in the *Second Notice,* FirstNet understands that States, like FirstNet, will potentially have gaps in information at the time of their RFP process, and subsequently at the time of their submission of an alternative plan. For instance, because States will not have negotiated a spectrum capacity lease with FirstNet upon the initial

[49] *See* Oxford Dictionary of English (3 ed. 2014), *http://www.oxforddictionaries.com/definition/english/plan* (last visited Aug. 30, 2015).

[50] *See* 47 U.S.C. 1442(e)(2)(A).

[51] *See* 47 U.S.C. 1422(e)(2).

[52] *See* 47 U.S.C. 1442(e)(1).

submission of their alternative plan, certain final terms within the States' own covered leasing agreements with their respective partners will likely not have been fully negotiated. FirstNet believes this should not preclude a State from submitting an alternative plan, so long as within the 180-day time period the State has progressed to the extent necessary to submit an alternative plan in accordance with the requirements described in section 1442(e)(3)(C)(i).

Accordingly, FirstNet makes the following conclusions regarding the State's development of an alternative plan:

1. FirstNet concludes that the phrase ''complete requests for proposals'' means that a State has progressed in such a process to the extent necessary to submit an alternative plan for the construction, maintenance, operation, and improvements of the RAN that demonstrates the technical and interoperability requirements in accordance with 47 U.S.C. 1442(e)(3)(C)(i).

2. FirstNet concludes that where a State fails to ''complete'' its RFP within the 180-day period pursuant to the Act, the State forfeits its ability to submit an alternative plan pursuant to 47 U.S.C. 1442(e)(3)(C), and the construction, maintenance, operations, and improvements of the RAN within the State shall proceed in accordance with the FirstNet proposed State plan for such State.

Analysis of and Responses to Comments Regarding the State's Development of an Alternative Plan

The majority of respondents agreed with FirstNet's conclusion that, due to the similar nature of the States' responsibility to ''complete requests for proposals'' and FirstNet's requirement to notify the States upon ''completion of the request for proposal process,'' States should similarly only need to progress to the point in its RFP process to be able to submit an alternative plan for the construction, maintenance, operation, and improvements of the RAN that also demonstrates the technical and interoperability requirements described in the FCC's evaluation criteria pursuant to section 1442(e)(3)(C)(i). Similarly, the majority of commenters agreed with FirstNet's conclusion that the Act's interest in timely network deployment compels the State and FirstNet to proceed in accordance with FirstNet's proposed State plan if the State is unable to submit an alternative plan within 180 days as required pursuant to section 1442(e)(3)(C)(i).

Several commenters, however, maintained that the 180-day timeline is too short of a period for a State to realistically complete its RFP process and that the State should not have to forfeit its ability to submit an alternative plan if it does not complete the RFP process within the 180 days. Several commenters seemed to suggest that States must be ''complete'' enough in their RFP process to provide information over and above that which FirstNet had concluded was required within the 180-day timeline.

Comment #39: Numerous commenters expressed their frustration at the short time periods established by the Act, with several suggesting that FirstNet extend the 180-day deadline based on certain factors determined by FirstNet regarding consultation activities.

Response: FirstNet was created by Congress and is bound by the statutory language contained within the Act. The Act explicitly provides for a 180-day period following the Governor's decision to opt-out to ''develop and complete requests for proposals for the construction, maintenance, and operation of the [RAN] within the State.'' [53] FirstNet has no ability to change the plain language of the Act and is not authorized to extend the 180-day time period.

FirstNet acknowledges the issues regarding timeframes raised in certain of the comments and therefore has concluded that such ''completion'' required pursuant to section 1442(e)(3)(B) is only required to the extent necessary to be able to submit an alternative plan for the construction, maintenance, operation, and improvements of the RAN that also demonstrates the technical and interoperability requirements in accordance with 47 U.S.C. 1442(e)(3)(C)(i).

Comment #40: Numerous respondents asserted that the State should not be required to forfeit its ability to submit an alternative plan if it fails to submit its alternative plan within the 180-day timeline.

Response: FirstNet disagrees with this statement based on the purpose and language of the Act. Throughout the Act, numerous references express the desire for timely network deployment.[54] In addition, the Act explicitly imposes timelines that a State must meet in order to proceed through the alternative plan process.[55]

The Act weighs a State's right to conduct its own RAN deployment in the State with public safety's need to expeditiously gain the benefit of interoperable communications across State borders. In doing so, it established a clear process relating to State assumption of RAN deployment. FirstNet does not have the authority to alter this statutory process and must adhere to the express language and intent of the Act to speed deployment of a nationwide broadband network for public safety. In keeping with the language and purpose of the Act, FirstNet concludes that where a State fails to ''complete'' its RFP in the 180-day period pursuant to the Act, the State forfeits its ability to submit an alternative plan in accordance with section 1442(e)(3)(C), which results in the State proceeding in accordance with the FirstNet-proposed State plan.

Comment #41: One commenter seems to confuse the State's forfeiture of its opportunity to assume RAN responsibilities with the supposition that FirstNet would be, in effect, forcing a State's first responders to subscribe to the NPSBN by proceeding with FirstNet's originally proposed State plan.

Response: FirstNet reiterates that the Act does not mandate public safety use of the NPSBN. Once FirstNet proceeds with the deployment of its proposed State plan, or a State takes on the RAN deployment and operation responsibility, all public safety entities across the country will have the choice whether to subscribe to the NPSBN.[56]

Comment #42: Several commenters maintained that FirstNet must continue to ensure it is providing States with as much information as possible as soon as possible due to the tight timeframes established within the Act.

Response: FirstNet, as previously stated, is committed to continuing its consultation activities and coordinating with the States as it develops and presents the State plans.

Comment #43: One commenter suggested that a State should reasonably be required to sufficiently develop and complete the RFPs during the 180-day period and advance in such process to the extent necessary to not only enable the State to meet the requirements of section 1442(e)(3)(C), but also those of section 1442(e)(3)(D).

Response: FirstNet appreciates the tight timeframes included within the Act and has taken practical steps to help ensure that a State has a reasonable opportunity to proceed with deploying its own RAN in the State. States are not

[53] *See* 47 U.S.C. 1442(e)(3)(B).

[54] *See, e.g.,* 47 U.S.C. 1426(b)(1)(C) (describing the need for existing infrastructure to ''speed deployment of the network''); *see also e.g.,* 47 U.S.C. 1426(b)(3) (including partnerships to ''speed deployment'' in rural areas).

[55] *See* 47 U.S.C. 1442(e)(2)–(3).

[56] *See generally* 47 U.S.C. 1428(a)(1).

required to know all details of their alternative plan, but instead to have progressed to a point to be able to present an alternative plan for the construction, maintenance, operation, and improvements of the RAN that is also able to demonstrate the technical and interoperability obligations required pursuant to section 1442(e)(3)(C)(i). FirstNet agrees with the respondent that a State must provide information specified in section 1442(e)(3)(D) prior to NTIA being able to complete its section 1442(e)(3)(D) comparisons pursuant to the Act and for the State to seek to enter into a spectrum capacity lease with FirstNet.[57] FirstNet concludes, however, that within the 180-day timeframe, the State must only be able to submit an alternative plan for the construction, maintenance, operation, and improvements of the RAN that also demonstrates the technical and interoperability requirements within section 1442(e)(3)(C)(i).[58]

Final Interpretations Regarding the Responsibilities of FirstNet and a State Upon a State Decision To Assume Responsibility for the Construction and Operation of Its Own RAN

Under 47 U.S.C. 1442(e)(3)(C)(iii), the FCC's decision to approve a State's alternative plan triggers the State's obligation to apply to NTIA to seek a spectrum capacity lease from FirstNet (while also allowing the State to apply for a grant to assist in the construction of the State's RAN). Several questions with respect to these provisions of the Act are discussed in the *Second Notice* regarding the implications and effects on FirstNet and a State of the FCC's decision to approve or disapprove a State's alternative plan.

Based on its analysis in the *Second Notice,* FirstNet makes the following conclusions regarding the responsibilities of FirstNet and a State upon a State's decision to assume responsibility for the construction and operation of its own RAN:

1. FirstNet concludes that once a plan has been disapproved by the FCC, subject only to the additional review described in 47 U.S.C. 1442(h), the opportunity for a State to conduct its own RAN deployment pursuant to 47 U.S.C. 1442(e) will be forfeited, and FirstNet shall proceed in accordance with its proposed plan for that State.

2. FirstNet concludes, following an FCC-approved alternative State RAN plan, it would have no obligation to construct, operate, maintain, or improve the RAN within such State.

3. FirstNet concludes that if a State, following FCC approval of its alternative plan, is unable or unwilling to implement its alternative plan in accordance with all applicable requirements, then FirstNet may assume, without obligation, RAN responsibilities in the State.

Analysis of and Responses to Comments Regarding the Responsibilities of FirstNet and a State Upon a State Decision To Assume Responsibility for the Construction and Operation of Its Own RAN

Commenters generally agreed with FirstNet's conclusions regarding the responsibilities of a State and FirstNet following the FCC's decision to approve or disapprove a State's alternative plan. Almost all respondents agreed that if the FCC were to disapprove a State's alternative plan, subject to the judicial review allowed in section 1442(h), the State would proceed according to FirstNet's proposed plan.[59] Most commenters agreed that once the FCC approves an alternative plan, the State itself must assume the obligation for the construction, operation, maintenance, and improvement of the RAN in such State, and acknowledged FirstNet's rationale for concluding its obligation to deploy a State plan would be extinguished.

Additionally, several commenters stated that it was their belief that FirstNet should provide assurances that it will ensure every State has NPSBN service offerings, whether such State opts-in or fails in its attempt to deploy and operate the RAN. On the other hand, one commenter cautioned FirstNet against adopting interpretations that would allow for the ''rescue of opt-out'' States without clarifying that such a scenario should not be seen by the States as a ''safety net.''

Comment #44: One respondent maintained that the State should not be required to forfeit its ability to conduct its own RAN deployment and proceed with the FirstNet-proposed State plan following an FCC decision to disapprove the State's alternative plan pursuant to section 1442(e)(3)(C)(iv).

Response: FirstNet disagrees with this statement based on the plain language of the Act. Section 1442(e)(3) explicitly states that ''[i]f the [FCC] disapproves [a State's alternative plan], the construction, maintenance, operation, and improvements of the network within the State *shall proceed in accordance with the plan proposed by [FirstNet].*'' [60] A State does have the right to appeal the FCC's decision to the U.S. District Court for the District of Columbia,[61] but the Act's language makes it clear that deployment within the State shall proceed according to FirstNet's proposed State plan following FCC disapproval of the alternative plan.

Comment #45: One commenter expressed that it would be beneficial to have an appeals process following the submission to the FCC, in instances where the State plan was not approved, through which the decision could be referred to an independent third party for adjudication.

Response: Section 1442(h) already specifically designates an appeals process with respect to the FCC's disapproval of an alternative plan, whereby ''[t]he United States District Court for the District of Columbia shall have exclusive jurisdiction to review a decision of the [FCC] pursuant to subsection (e)(3)(C)(iv).'' [62] Any additional appeals processes would contradict the express language of the Act that the U.S. District Court for the District of Columbia has ''exclusive jurisdiction'' to review the FCC's decision to disapprove a State's alternative plan, as well as simply add to the likely substantial delays that would result in the NPSBN deployment within the respective States.

Comment #46: Several commenters asserted that FirstNet's central obligation pursuant to the Act is to ensure the deployment of the NPSBN in every State, and that, even if a State gains all necessary approvals to implement its alternative plan and eventually fails, FirstNet's obligation to deploy the network nationwide is never extinguished and must proceed according to the FirstNet-proposed State plan.

Response: Each Governor is given the option to decide to participate in FirstNet's proposed State plan or to progress through a statutorily-mandated process to assume the obligation for constructing, maintaining, operating, and improving its own State RAN.[63] This process can infuse significant delays in the deployment based on the statutorily-mandated timeframes for the Governor's decision and the development of an alternative State plan by the State.[64] Further, the Act provides

[57] *See* 47 U.S.C. 1442(e)(3)(D).

[58] *See* 47 U.S.C. 1442(e)(3)(B), (C)(i).

[59] *See* 47 U.S.C. 1442(e)(3)(C)(iv).

[60] 47 U.S.C. 1442(e)(3)(C)(iv) (emphasis added).

[61] *See* 47 U.S.C. 1442(h).

[62] *See id.*

[63] *See* 47 U.S.C. 1442(e).

[64] *See* 47 U.S.C. 1442(e)(2), (3)(C)(i) (providing that the Governor has 90 days to make a decision on State RAN deployment and 180 days to complete

Continued

no explicit timelines for the FCC to review and approve or disapprove of an alternative plan, and affords an additional unspecified period of time to appeal any disapproval to the U.S. District Court for the District of Columbia.[65]

Given the timeframes required by the Act to reach the point of the approval of an alternate plan by the FCC, it is critical that thereafter FirstNet and its eventual RFP partner(s) are able to rely on the State decision to proceed with RAN deployment so FirstNet can appropriately plan for the deployment throughout the rest of the nation. FirstNet cannot be in a position to further delay the nationwide availability of the NPSBN due to a single State's inability or unwillingness to deploy the RAN within that State. In addition, the Act does not provide a mechanism requiring FirstNet to assume responsibility for local RAN deployment after a State has elected, and been approved, to do so. Indeed, to the contrary, Congress indicated its clear intent in requiring FirstNet to proceed with its State plan only in the case where a State's alternative plan was disapproved by the FCC. Congress could have just as easily included a requirement that FirstNet proceed with a State plan if a State was unable or unwilling to proceed under its alternative plan. However, we believe Congress created a balance in favor of certainty and speed to deployment, which is consistent with the detailed process and steps Congress implemented in the Act to ensure alternative State plans initially met the necessary criteria for State deployment and operation of the RAN.[66]

Therefore, FirstNet reiterates its conclusion that, following an FCC-approved alternative plan, it would have no obligation to construct, operate, maintain, or improve the RAN within such State, but if the State becomes unable or unwilling to implement its alternative plan in accordance with all applicable requirements, then FirstNet may assume, without obligation, the RAN responsibilities in the State.

D. Customer, Operational, and Funding Considerations Regarding State Assumption of RAN Construction and Operation

Customer Relationships in States Assuming RAN Construction and Operation

The Act does not expressly define which customer-facing roles are assumed by a State or FirstNet with respect to public safety entities in States that have assumed responsibility for RAN construction and operation. Generally speaking, all wireless network services to public safety entities will require technical operation of both the RAN, operated by the State in this case, and the core network, operated by FirstNet. The Act charges FirstNet with ensuring the establishment of the NPSBN, including the deployment of the core network, but provides States an opportunity, subject to certain conditions, to conduct the deployment of a RAN in a State.[67] A core network, for example, would typically control critical authentication, mobility, routing, security, prioritization rules, and support system functions, including billing and device services, along with connectivity to the Internet and public switched network. Conversely, the RAN would typically dictate, among other things, the coverage and capacity of last mile wireless communication to customer devices and certain priority and preemption enforcement points at the wireless interface of the network. The allocation of these technical and operational functions, however, does not entirely dictate who assumes public safety customer-facing roles, such as marketing, execution of customer agreements, billing, maintaining service responsibility, and generating and using fees from public safety customers. Thus, the conclusions below relate to FirstNet and the State's respective roles and approach with regard to customer relationships in States assuming responsibility for RAN construction and operation in that State.

1. FirstNet concludes that the Act provides sufficient flexibility to accommodate many types of customer relationships with public safety entities for States assuming RAN responsibility so long as the relationships meet the interoperability and self-sustainment goals of the Act.

2. FirstNet concludes that the Act does not require that States assuming RAN deployment responsibilities be the customer-facing entity entering into agreements with and charging fees to public safety entities in such States.

3. FirstNet concludes that the Act does not preclude States assuming RAN deployment responsibilities from charging subscription fees to public safety entities if FirstNet and such States agree to such an arrangement in the spectrum capacity lease.

4. FirstNet concludes that the Act provides sufficient flexibility to allow the determination of whether FirstNet or a State plays a customer-facing role to public safety entities in a State assuming RAN responsibilities, to be the subject of operational discussions between FirstNet and the State in negotiating the terms of the spectrum capacity lease.

5. FirstNet concludes that it will maintain a flexible approach to such functions and interactions in order to provide the best solutions to each State so long as the agreed upon approach meets the interoperability and self-sustainment goals of the Act.

Analysis of and Responses to Comments on Customer Relationships in States Assuming RAN Construction and Operation

Summary: All commenters generally agreed with FirstNet's interpretations relating to the nature of customer relationships in States assuming RAN construction and operation. Commenters concurred with the interpretation that by maintaining flexibility in determining whether FirstNet or States will be the customer-facing entity, it allows States to tailor their operations to meet their individual State public safety broadband needs, while still ensuring the achievement of the interoperability and self-sustainment goals of the Act.

Final Interpretation of FirstNet Analyzing Funding Considerations as Part of Its Determination To Enter Into a Spectrum Capacity Lease

FirstNet has number of funding sources, including: (1) Up to $7 billion in cash; (2) user or subscriber fees; (3) fees from excess network capacity leases that allow FirstNet to lease capacity not being used by public safety to commercial entities under covered leasing agreements; and (4) lease fees related to network equipment and infrastructure.[68] Each of these funding sources is critical to offset the massive costs of building, operating, and maintaining the NSPBN envisioned in the Act and in meeting the self-sustainability requirements placed on FirstNet pursuant to the Act.

However, States seeking and receiving approval of alternative RAN plans could

the RFP process if the State is seeking to conduct its own RAN deployment).

[65] *See* 47 U.S.C. 1442(h).

[66] *See* U.S.C. 1442(e)(3)(C)(iv) (stating where the FCC disapproves an alternative plan, the State proceeds according to FirstNet's proposed plan); 47 U.S.C. 1442(e)(3)(D) (failing to assert that a State must proceed with the FirstNet proposed plan when a FCC-approved plan subsequently fails to demonstrate the requirements to NTIA pursuant to Section 1442(e)(3)(D) to seek a spectrum capacity lease from FirstNet).

[67] *See* 47 U.S.C. 1422(a), (e).

[68] *See generally* 47 U.S.C. 1428(a), 1457(b)(3).

materially affect FirstNet's funding sources and thus its ability to serve public safety, particularly in rural States. More precisely, a State that assumes RAN deployment responsibilities could benefit from, or supplant, these funding sources, by generating and retaining amounts in excess of that necessary to reasonably maintain the particular State RAN through monetization of FirstNet's licensed spectrum. By doing so, the excess value above that reasonably needed to operate and maintain the RAN would no longer be available to help ensure that nationwide deployment, particularly in higher cost rural areas, will occur. This undermines the intent of the Act and the express requirement for FirstNet to deploy in rural areas as part of each phase of implementation.[69]

Accordingly, FirstNet concludes, based on the language and the intent of the Act, that Congress did not intend to permit alternative RAN plans that inefficiently utilize scarce spectrum resources to hinder the nationwide deployment of the NPSBN by depriving it of needed financial support. FirstNet further concludes that it must thus consider the effect of any such material inefficiencies, among other things, on the NSPBN in determining whether, and under what terms, to enter into a spectrum capacity lease.

Congress's intent in this regard is informed by 47 U.S.C. 1442(e)(3)(D) requiring a State that wishes to assume RAN responsibilities to demonstrate ''the cost-effectiveness of the State plan'' when applying to NTIA not just for grant funds, but also for spectrum capacity leasing rights from FirstNet, which are necessary for the implementation of a State RAN. Independent of NTIA's determination in assessing such an application, FirstNet, as the licensee of the spectrum and an independent authority within NTIA, must ultimately decide on what terms to enter into a spectrum capacity lease with a State. The conclusions below relate to FirstNet's role and responsibilities in negotiating a spectrum capacity lease with a State seeking to assume responsibilities for deploying its RAN.

1. FirstNet concludes, in fulfilling its duties and responsibilities under the Act, it can and must take into account funding considerations, including the ''cost-effectiveness'' of an alternative state plan as it may impact the national deployment of the NPSBN, in determining whether and under what terms to enter into a spectrum capacity lease with a State.

2. FirstNet concludes as part of its cost-effectiveness analysis in determining whether and under what terms to enter into a spectrum capacity lease, it (i) must consider the impact of cost-inefficient alternative RAN plans, including inefficient use of scarce spectrum resources, on the NPSBN, and (ii) may require that amounts generated within a State in excess of those required to reasonably sustain the State RAN, be utilized to support the Act's requirement to deploy the NPSBN on a nationwide basis.

3. FirstNet concludes as part of its cost-effectiveness analysis it must consider State reinvestment and distribution of any user fees assessed to public safety entities or spectrum capacity revenues in determining whether and under what terms to enter into a spectrum capacity lease.

Analysis of and Responses to Comments on Funding Considerations Part of Determination To Enter Into a Spectrum Capacity Lease

Summary: Commenters generally agreed with these interpretations emphasizing, for example, that it would be entirely consistent with the Act for FirstNet to take into account its funding considerations, among other things, and impose conditions on such spectrum capacity leases to ensure that revenue from excess capacity arrangements and subscriber fees will be utilized in a manner that continues to facilitate the deployment of the NSPBN.

Certain commenters either disagreed with, or provided recommendations for, implementing these interpretations, particularly regarding whether and how FirstNet can and must take into account funding considerations, including the ''cost-effectiveness'' of the State plan, in order to guarantee the viability of a broadband network dedicated to public safety across the nation.

Comment #47: One commenter reasoned that FirstNet's proposed interpretation is unsupported by the Act's plain language, and potentially conflicts with existing federal authority over States.

Response: FirstNet disagrees that the interpretation is unsupported by the plain language of the Act. The Act directs the FCC to reallocate and grant a license to FirstNet for the use of the 700 MHz D block spectrum and existing public safety broadband spectrum.[70] FirstNet, as the designated licensee of the spectrum pursuant to the Act, has a statutory obligation to ensure the establishment of an interoperable, *nationwide* public safety broadband network.[71] To satisfy this obligation, FirstNet has been given broad authority to take actions it determines necessary, appropriate, or advisable to accomplish its mission.[72] As discussed in the *Second Notice,* FirstNet has determined that it must ensure the efficient use of each of its limited funding resources in order to offset the massive costs to build, operate, and maintain the NSPBN envisioned in the Act and also to meet the statutory self-sustainability requirement imposed on FirstNet pursuant to the Act.

To assist FirstNet in protecting critical financial resources, the Act requires, among other things, a State seeking to assume RAN responsibilities to demonstrate ''the cost-effectiveness of the State plan'' when applying to NTIA for spectrum capacity leasing rights from FirstNet, which are necessary for the implementation of a State RAN.[73] Consistent with the intent of the Act to ensure the nationwide deployment, FirstNet must consider the cost-effectiveness of the alternative State plan on that nationwide deployment. Indeed, independent of NTIA's determination in assessing such an application, FirstNet, as the designated licensee of the spectrum pursuant to the Act and an independent authority within NTIA, must ultimately decide whether and pursuant to what terms to enter into a spectrum capacity lease with a State.[74] Accordingly, FirstNet has determined that it is necessary to take into account funding considerations, including the ''cost-effectiveness'' of an alternative state plan, and its impact on FirstNet's ability to deploy the national network, in determining whether and under what terms to enter into a spectrum capacity lease.

Comment #48: Several commenters reasoned that the proposed interpretation either acts as a tax or assigns additional costs to a State that

[69] *See* 47 U.S.C. 1426(b)(3).

[70] *See* 47 U.S.C. 1421.

[71] *Id.*

[72] *See* 47 U.S.C. 1426(a)(6).

[73] *See* 47 U.S.C. 1442(e)(3)(D).

[74] We note that FirstNet's interpretation of this provision and its determination with regard to its duties based on the State's proposed demonstration is independent of and does not limit NTIA. To the extent the ''spectrum capacity lease'' described in section 1442(e)(3)(C)(iii)(II) is a lease of the spectrum itself, rather than capacity on the network, under applicable FCC rules, the FCC ''will allow parties to determine precise terms and provisions of their contract'' consistent with FirstNet's obligations as a licensee under such rules. *See* Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets, WT Docket No. 00–230, *Report and Order and Further Notice of Proposed Rulemaking,* FCC 03–113, 18 FCC Rcd 20604, 20637 (2003).

has assumed responsibility for RAN deployment.

Response: FirstNet disagrees that its interpretation acts as a tax or results in any actual or additional costs to a State that assumes deployment for a RAN in the State. Rather, as discussed in the *Second Notice,* FirstNet's interpretations ensure that States are not able to retain excess value not reasonably needed for the RAN in that State, and are intended to protect the limited resources provided by Congress to ensure the establishment of a *nationwide* broadband network for public safety.

Comment #49: Several commenters noted generally that the terms of a spectrum capacity lease are vital to preserving the opportunity for a State to choose to conduct its own deployment of a RAN, and accordingly, the terms of the spectrum capacity lease agreement, although negotiated, should be conducted in an open and transparent manner. Such commenters also asserted that the terms should be reasonable and known at the same time FirstNet delivers its State plan in order to maintain a partnership between FirstNet and the States.

Response: FirstNet acknowledges the comments and will consider them, as appropriate, in the development of any processes or requirements related to a spectrum capacity lease.

Comment #50: Three commenters expressed concern that FirstNet would abuse its authority under this interpretation by leveraging its control of the spectrum to demand virtually any concession it wanted during the negotiation of a spectrum capacity lease, thereby creating a set of circumstances in which the opportunity for a State to conduct is own RAN deployment pursuant to the Act is not a meaningful opportunity.

Response: FirstNet recognizes that the Act strikes a balance between establishing a nationwide network and providing States an opportunity, under certain conditions, to maintain and operate the RAN portion of the network in their States. Accordingly, FirstNet intends to act in good faith with each of the States to explore ''win-win'' solutions with States desiring to assume RAN responsibilities, including in scenarios where potential revenue would materially exceed RAN and related costs in a State consistent with the requirements and intent of the Act.

Comment #51: One commenter, although recognizing FirstNet's responsibility to maximize the build out of a network in all States, disagreed that a State's alternative RAN plan, once approved by the FCC, should be subject to spectrum capacity lease considerations that are outside the geographical area of the State.

Response: The Act expressly charges FirstNet with ensuring the establishment of a *nationwide* public safety broadband network.[75] To satisfy this mandate, FirstNet must consider and account for the use of the limited resources provided it in order to accomplish this mission. This includes ensuring that the scarce spectrum resources provided for the nationwide network are not used in a materially inefficient manner that could negatively impact the deployment of the entire network. Specifically, FirstNet has a duty to consider the effect of any such inefficiencies on, among other things, more rural States, and on the larger FirstNet program, in determining whether, and under what terms, to enter into a spectrum capacity lease.

Comment #52: One commenter stated that the benefit of requiring ''opt-out'' urban States to provide ''excess'' revenues to FirstNet for rural build out nationwide should not apply to a rural State that may want to take responsibility for its own RAN deployment.

Response: FirstNet's analysis of funding considerations must equally apply to all States that are able to generate value in excess of the reasonable costs of operating and maintaining the RAN when electing to assume RAN responsibility within the State, so as to ensure sufficient resources are available for the national deployment of the NPSBN. However, we acknowledge that likely only a limited number of jurisdictions will generate such excess value, which would be available to help support deployment, for example, in higher cost, rural areas.

Comment #53: One commenter stated it does not support FirstNet's interpretation and proposed that any ''cost-effectiveness'' evaluation of a State plan must begin and end with the effect on the State and argued that the Governor's obligation is to provide the best possible, most cost-effective, solution for that State's residents.

Response: FirstNet agrees that pursuant to the Act, a State Governor has the right to determine whether it is in the best interest of a State to participate in the State RAN plan as proposed by FirstNet, or instead seek to conduct the deployment of its own RAN within the State. Accordingly, a Governor may choose to independently evaluate whether it is more cost-effective to participate in the State RAN plan as proposed by FirstNet or conduct its own deployment of a RAN in the State. In contrast, FirstNet has an obligation to ensure the establishment of a nationwide network and must take into consideration the interests of all States rather than only a single State. Accordingly, FirstNet, based on the reasoning in the *Second Notice,* has determined that as a part of its decision to enter into a spectrum capacity lease it must take into account the cost-effectiveness of the proposed alternative State plan, including the impact of the plan on the nationwide network.

Comment #54: One commenter recommended that the reinvestment analysis should define more clearly the network to ensure RANs that service both public safety entities and secondary users should be targeted first for reinvestment instead of being limited to a RAN for public safety only.

Response: FirstNet acknowledges this recommendation and will consider it as any applicable decisions are developed on the matter.

Comment #55: One commenter noted that any lease of excess capacity needs to recognize that the amount of such excess may very well vary by State and decrease over time, citing several studies that indicated 20 MHz of spectrum will be needed, and in some very large incidents, may not be totally sufficient for public safety use. Therefore, the commenter suggested that the amount of supplemental funding that can be attained from covered leasing agreements should follow a determination of the spectrum capacity required by public safety instead of having the amount of spectrum available to public safety be determined by the additional funding beyond the $7 billion needed for the network.

Response: FirstNet acknowledges this recommendation and will consider it as any applicable decisions are developed on the matter.

Comment #56: One commenter requested clarification on whether the preliminary interpretation would mean that no excess revenues will ever be allowed to offset, in whole or part, public safety subscriber fees or if all of those revenues will only be reinvested back into the network to maintain or expand infrastructure.

Response: FirstNet's interpretation does not expressly foreclose the potential for excess revenues to offset, in whole or part, public safety user or subscriber fees provided such reinvestment comports with the requirements of 47 U.S.C. 1428(d), 1442(g).

Comment #57: Three commenters, although supporting the goal of ensuring build out in rural areas, requested more

[75] 47 U.S.C. 1422(a).

clarification on the general scope of the FirstNet spectrum capacity lease requirements, including the scope of the proposed ''cost-effectiveness'' analysis.

Response: FirstNet acknowledges the comments and will consider them, as appropriate, in the development of any processes or requirements related to a spectrum capacity lease.

Comment #58: One commenter indicated that NTIA, and not FirstNet, has the ultimate decision-making authority over the entry of spectrum capacity leases with States assuming RAN responsibilities. As support, the commenter referenced 47 U.S.C. § 1442(e)(3)(C)(iii), which provides that if the Commission approves a State plan, the State ''shall apply to the NTIA to lease spectrum capacity from the First Responder Network Authority.'' Accordingly, the Commenter contended that only NTIA has the authority to enter into spectrum capacity leases with opt-out States.

Response: FirstNet disagrees with the commenter and reiterates that independent of NTIA's determination in assessing a spectrum capacity lease application, FirstNet, as the licensee of the spectrum pursuant to section 1421 and an independent authority within NTIA, must ultimately decide on what terms to enter into a spectrum capacity lease with a State, and in doing so, evaluate, for example, the State's demonstration of cost-effectiveness of the State's alternative plan on the national deployment per section 1442(e)(3)(D)(ii). The relevant language regarding spectrum capacity leases for States that assume RAN responsibility can be found at section 1442(e)(3)(C)(iii)(II), which provides that once the FCC approves an alternative State plan, the State ''shall *apply* to the NTIA to lease spectrum capacity *from the First Responder Network Authority.*'' [76] We emphasize language in this provision noting that the State would need to lease spectrum capacity *from* FirstNet. The Act is clear that the license for the public safety broadband spectrum has been granted exclusively to FirstNet.[77] As the exclusive licensee of the spectrum, FirstNet alone can negotiate and enter into an agreement to lease this spectrum. In addition, section 1442(e)(3)(D) sets forth the criteria a State must demonstrate in order to obtain spectrum capacity leasing rights. Accordingly, reading sections 1421, 1442(e)(3)(C), and 1442(e)(3)(D) of the Act together, the statute provides that a State assuming RAN responsibility must (1) submit an application to NTIA in order to lease spectrum capacity, (2) demonstrate to NTIA compliance with all applicable criteria, including the cost-effectiveness of the alternative plan on the nationwide deployment, and (3) negotiate an agreement to lease this spectrum capacity from FirstNet, prior to being authorized to conduct RAN deployment in that State.

Reinvestment of User or Subscriber Fees

FirstNet has interpreted that the Act provides flexibility for FirstNet and a State assuming RAN responsibilities to reach an agreement regarding who serves as the customer facing entity and ultimately receives such user or subscription fees under the spectrum capacity lease, with respect to the user fees generated from public safety customers in a State. In accordance with the structure and purposes of the Act, which requires that the NSPBN be self-funded, and includes specific provisions requiring reinvestment of revenues in the network, FirstNet makes the following conclusions relating to the use of user or subscription fees assessed and collected by a State assuming responsibility for deploying the RAN:

1. FirstNet concludes that the Act requires that States assuming RAN deployment responsibilities and charging user or subscription fees to public safety entities must reinvest such fees into the network.

2. FirstNet concludes it could impose a reinvestment restriction within the terms of a spectrum capacity lease with a State.

Analysis of and Responses to Comments on Reinvestment of User or Subscription Fees

Summary: Commenters generally agreed with the interpretation that user or subscriptions fees must be reinvested in the network, recognizing that to achieve network sustainment, all fees, revenues, etc. would need to be reinvested into the network. The dissenting commenters, as documented below, did not typically disagree that the funds must be reinvested in the network, but rather wanted to limit the reinvestment of the funds solely to RAN construction, operation, and maintenance in the State where the fees were assessed rather than requiring reinvestment to include the nationwide network.

Comment #59: One commenter disagreed with the proposed interpretation that FirstNet could consider or impose a reinvestment restriction as part of a spectrum capacity lease, stating that such a conclusion is not supported by the plain language of the Act.

Response: See the response to Comment #47 discussing the ability of FirstNet to negotiate the specific terms and conditions of a spectrum capacity lease.

Comment #60: One commenter disagreed with the proposed interpretation that a State choosing to conduct its own RAN deployment must pay a part of its subscriber fees to FirstNet, rather than retain and reinvest those funds directly in the State RAN.

Response: FirstNet's interpretations leave flexibility for a State to generate or receive user or subscription fees from public safety customers and reinvest such fees into the RAN in the State. However, the specific arrangement will ultimately depend on many factors, including both a State's proposed reinvestment of such fees and the cost-effectiveness considerations regarding the distribution of such fees that will be evaluated as part of any negotiation between FirstNet and a State seeking to enter into such a spectrum capacity lease. As discussed in the *Second Notice,* subscriber fees may ultimately exceed those amounts necessary to deploy a robust RAN in any one State. Accordingly, if the Act is interpreted to allow excess funds to be reinvested only in a specific State, there is a built-in incentive for a few States to conduct RAN deployment and retain, for reinvestment in that State, fees that could materially reduce FirstNet coverage and services in other States, including States with more rural areas. FirstNet believes, as a general matter, that Congress did not intend for a few States to be able to withhold material funding for all other States pursuant to the Act. Such an incentive structure, even if reinvestment in the State network were always required in States assuming RAN responsibilities, could result in networks that greatly exceed public safety requirements in a few such States and networks that do not meet public safety requirements and the goals of the Act in the vast majority of States. Accordingly, as concluded above, FirstNet, as part of its cost-effectiveness analysis, must consider a State's reinvestment and distribution of any user fees assessed to public safety entities as part of the negotiated terms of any spectrum capacity lease between FirstNet and the State.

Comment #61: One commenter suggested the provisions for reinvestment should define more clearly the network to ensure the RAN that services dual purposes (*i.e.,* both public safety entities and secondary users) should be targeted first for reinvestment.

[76] 47 U.S.C. 1442(e)(3)(C)(iii) (emphasis added).

[77] 47 U.S.C. 1421.

Response: The RAN, whether deployed by FirstNet or a State, will be capable of being utilized by both public safety entities and secondary users. Thus, any funds reinvested in a State RAN will likely positively impact both public safety and secondary users. However, public safety entities are intended to be the primary users of the network. Therefore, to the extent that a RAN requires special modifications specifically for, or on behalf of public safety entities, such modifications will likely take priority over general investments in the RAN. Nevertheless, FirstNet anticipates gaining a better understanding of these specific needs and priorities as it continues both its ongoing consultation with its various stakeholders as well as part of any negotiation between FirstNet and a State to enter into a spectrum capacity lease.

Comment #62: One commenter disagreed with FirstNet's interpretation of the Act, expressing concern that reinvestments of subscriber fees is a tax on public safety responders and stating that any charges above and beyond what is necessary to maintain and improve a State's RAN should be returned to that State's public safety community in the form of rate reductions, training, and better equipment.

Response: See the responses to Comment #48 and Comment #56 above.

Reinvestment of Revenues From State Covered Leasing Agreements/Public-Private Partnerships

The Act includes certain provisions addressing the reinvestment of covered leasing agreement fees for States assuming RAN deployment opportunities that have both received approval from NTIA and entered into a spectrum capacity lease with FirstNet.[78] We analyzed, in the *Second Notice,* the parallels between FirstNet and the State provisions addressing the reinvestment of such fees pursuant to the Act. For example, section 1428(d) requires FirstNet to reinvest those amounts received from the assessment of fees pursuant to section 1428 in the NPSBN by using such funds only for constructing, maintaining, operating, or improving the network.[79] Parallel to section 1428(d), section 1442(g)(2) requires that any amounts gained from a covered leasing agreement between a State conducting its own deployment of a RAN and a secondary user must be used only for constructing, maintaining, operating, or improving the RAN of the State.[80]

Section 1428(a)(2) authorizes FirstNet to charge lease fees related to covered leasing agreements. Other than such agreements, however, FirstNet is not expressly authorized to enter into other arrangements involving the sale or lease of network capacity. In potential contrast, section 1442(g)(1) precludes States from providing ''commercial service to consumers or offer[ing] wholesale leasing capacity of the network within the State *except directly through public-private partnerships for construction, maintenance, operation, and improvement of the network within the State.*'' [81] Section 1442(g)(2), entitled ''Rule of construction,'' provides that ''[n]othing in this subsection shall be construed to prohibit the State and a secondary user from entering into a covered leasing agreement.'' [82]

To reconcile the differences in these provisions, FirstNet, in accordance with its analysis in the *Second Notice,* makes the following interpretations relating the potential treatment of a covered leasing agreement and a public-private partnership for construction, maintenance, operation, and improvement of the network:

1. FirstNet concludes that, in practical effect, the literal statutory differences between a covered leasing agreement and public-private partnership as used in the Act result in no substantive difference between the Act's treatment of FirstNet and States that assume RAN responsibility.

2. FirstNet concludes that any revenues from public-private partnerships, to the extent such arrangements are permitted and different than covered leasing agreements, should be reinvested into the network and that the reinvestment provision of 47 U.S.C. § 1442(g) should be interpreted to require such reinvestment.

Analysis of and Responses to Comments on Reinvestment of Revenues From State Covered Leasing Agreements/Public-Private Partnerships

Commenters generally supported the interpretation, agreeing that through the provisions of and overall framework and policy goals of the Act, Congress intended that any revenues from public-private partnership, to the extent such arrangements are permitted and different than covered leasing agreements, should be subject to the reinvestment requirements of the Act. However, a few commenters, as discussed below, disagreed with the interpretation.

Comment #63: One commenter suggested the proposed interpretation regarding public-private partnerships is too narrow and will only serve to inhibit creative, customized solutions for RAN build out and maintenance within a State. Specifically, the commenter noted that the Act allows FirstNet to lease spectrum capacity to commercial providers who are free to offer commercial service and to profit from the arrangement, and likewise, the Act should be interpreted to permit opt-out States in connection with selected partners to have this same economic opportunity.

Response: FirstNet disagrees that its interpretation inhibits or limits customized solutions for RAN build out and maintenance within a State. The Act allows both FirstNet and States that have received approval of an alternative plan and entered into a spectrum capacity lease with FirstNet to enter into covered leasing agreements.[83] A covered leasing agreement, as the only instrument in the Act that permits access to network capacity on a secondary basis for non-public safety services, is a fundamental tool to attract entities to assist in the construction, management, and operation of the NPSBN, including State RANs. Consequently, a State that enters into a covered leasing agreement with a secondary user would be afforded the same benefits that are available to FirstNet pursuant to section 1428(a)(2)(B), including permitting the secondary user access to network capacity on a secondary basis for non-public safety services. Similarly, the only limitations on the covered leasing agreements between a State and secondary user would be those described in the Act, including reinvestment of such revenues in the RAN, and the terms and conditions agreed upon by FirstNet and the State as part of the spectrum capacity lease.[84] Thus, the same potential economic opportunity exists for States assuming RAN responsibilities as for FirstNet nationally, including rural States, to develop partnerships with broadband providers, local telecommunications providers, or other private sector entities within such States.

Comment #64: One commenter provided a general comment about covered leasing agreements and public-private partnerships, stating that the negotiating entity should seek to maximize the profit it can obtain from the 700 MHz spectrum allotted to public safety by leasing the spectrum capacity

[78] 47 U.S.C. 1442(g).

[79] 47 U.S.C. 1428(d).

[80] 47 U.S.C. 1442(g)(2).

[81] 47 U.S.C. 1442(g)(1) (emphasis added).

[82] 47 U.S.C. 1442(g)(2).

[83] *See* 47 U.S.C. 1428(a), 1442(g)(2).

[84] *See id.*

to secondary users on a statewide, regional, or national basis—whichever arrangement is most profitable.

Response: FirstNet agrees that it should evaluate various funding and deployment options in order to help speed deployment and ensure the establishment of a self-sustaining broadband network dedicated to public safety throughout the nation.

Comment #65: One commenter suggested that, although revenue generated from a covered leasing agreement is an important financial contribution to the construction and maintenance of the nationwide network, FirstNet should not allow the promise of secondary leasing agreements to single-handedly drive its strategic decisions.

Response: FirstNet acknowledges the comment and intends to analyze and determine the most efficient and effective way to utilize its various funding streams to ensure the deployment and operation of a nationwide broadband network for public safety.

Comment #66: One commenter suggested that State law, not FirstNet, should determine the ability of an opt-out State to profit from public-private partnerships or covered leasing agreements.

Response: The Act authorizes States to enter into covered leasing agreements with secondary users through public-private arrangements and establishes the parameters of those arrangements.[85] Indeed, the Act explicitly limits the use of any revenue gained by a State through a covered leasing agreement to constructing, maintaining, operating, or improving the RAN of that State.[86] Similarly, FirstNet has also concluded that section 1428(d), authorizing a State to enter into public-private partnerships, was intended by Congress to be read consistently, to the extent such an arrangement is considered something different from a covered leasing agreement, so as to ensure ongoing reinvestment of all revenues into the network. This is consistent with the overall purpose and intent of the Act to ensure the deployment and operation of the NPSBN.

Dated: October 15, 2015.

Jason Karp,

Chief Counsel (Acting), First Responder Network Authority.

[FR Doc. 2015–26622 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–TL–P

[85] *See* 47 U.S.C. 1442(g)(2).

[86] *See id.*

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket Number: 140821696–5908–04]

RIN 0660–XC012

First Responder Network Authority; Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012

AGENCY: First Responder Network Authority, National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice; final interpretations.

SUMMARY: The First Responder Network Authority (''FirstNet'') publishes this *Notice* to issue final interpretations of its enabling legislation that will inform, among other things, forthcoming requests for proposals, interpretive rules, and network policies. The purpose of this Notice is to provide stakeholders FirstNet's interpretations on many of the key preliminary interpretations presented in the proposed interpretations published on September 24, 2014.

DATES: Effective October 20, 2015.

FOR FURTHER INFORMATION CONTACT: Eli Veenendaal, First Responder Network Authority, National Telecommunications and Information Administration, U.S. Department of Commerce, 12201 Sunrise Valley Drive, M/S 243, Reston, VA 20192; 703–648–4167; or *elijah.veenendaal@firstnet.gov*.

SUPPLEMENTARY INFORMATION:

I. Introduction and Background

The Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. 112–96, Title VI, 126 Stat. 256 (codified at 47 U.S.C. 1401 *et seq.*)) (the ''Act'') established the First Responder Network Authority (''FirstNet'') as an independent authority within the National Telecommunications and Information Administration (''NTIA''). The Act establishes FirstNet's duty and responsibility to take all actions necessary to ensure the building, deployment, and operation of a nationwide public safety broadband network (''NPSBN'').[1]

One of FirstNet's initial steps in carrying out this responsibility under the Act is the issuance of open, transparent, and competitive requests for proposals (''RFPs'') for the purposes of building, operating, and maintaining the network. We have sought—and will continue to seek—public comments on many technical and economic aspects of these RFPs through traditional procurement processes, including requests for information (''RFIs'') and potential draft RFPs and Special Notices, prior to issuance of RFPs.[2]

As a newly created entity, however, we are also confronted with many complex legal issues of first impression under the Act that will have a material impact on the RFPs, responsive proposals, and our operations going forward. Generally, the Administrative Procedure Act (''APA'')[3] provides the basic framework of administrative law governing agency action, including the procedural steps that must precede the effective promulgation, amendment, or repeal of a rule by a federal agency.[4] However, 47 U.S.C. 1426(d)(2) provides that any action taken or decision made by FirstNet is exempt from the requirements of the APA.

Nevertheless, although exempted from these procedural requirements, on September 24, 2014, FirstNet published a public notice entitled ''Proposed Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012'' (hereinafter ''the *First Notice*''),[5] seeking public comments on preliminary interpretations, as well as technical and economic issues, on certain foundational legal issues to help guide our efforts in achieving our mission.

The purpose of this *Notice* is to provide stakeholders notice of the final legal interpretations on many of the key preliminary interpretations presented in the *First Notice*. Additional background and rationale for this action and explanations of FirstNet's interpretations were included in the *First Notice* and are not repeated herein. The section immediately below labeled ''Final Interpretations'' summarizes FirstNet's final interpretations with respect to the *First Notice*. Thereafter, the section labeled ''Response to Comments'' summarizes the comments

[1] 47 U.S.C. 1426(b).

[2] The pronouns ''we'' or ''our'' throughout this *Notice* refer to ''FirstNet'' alone and not FirstNet, NTIA, and the U.S. Department of Commerce as a collective group.

[3] *See* 5 U.S.C. 551–59, 701–06, 1305, 3105, 3344, 5372, 7521.

[4] *See* 5 U.S.C. 551–559. The APA defines a ''rule'' as ''the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency and includes the approval or prescription for the future of rates, wages, corporate or financial structures or reorganizations thereof, prices, facilities, appliances, services or allowances therefor or of valuations, costs, or accounting, or practices bearing on any of the foregoing.'' 5 U.S.C. 551(4).

[5] 79 FR 57058 (September 24, 2014).

Consultation Q&A

The following questions were given to FirstNet during Florida's consultation on December 12, 2015.

Project/Consultation related

1. What outcome does FirstNet seek from the state consultation process?

2. Where is the FirstNet project plan?

    - Do you have a project schedule?

    - What are the milestones of the project?

    - What is the timetable for FirstNet Service Availability?

3. What are the roadblocks that are preventing Florida from moving to SLIGP phase II activities?

    - *Revised budget has been submitted*

Technical, Design and Roll-out

- Does FirstNet plan on one-size-fits all Core and RAN design?

- When will FirstNet release a high level or conceptual diagram of the network architecture?

- What is the scope of the Core and the RAN?

Consultation Q&A (cont'd)

- How does FirstNet intend to meet or exceed current and future capabilities offered by the private sector now?

- Where will data from the Core(s) be stored? Will the state retain control of this data? Who will own the data and what public record law will apply to the data?

- Does FirstNet plan on operating an application store similar to Google Play or the Apple App store? Will FirstNet create standards for applications to run across the network?

- Will the State have the opportunity to decide or be involved in the decision of how much excess spectrum is allocated for secondary usage?

- Does FirstNet envision an opt-in scenario where a State could build and operate its own Core that connects to the FirstNet national core?

- What is FirstNet's definition of local control?

- What is FirstNet's definition of rural?
    - *Any area that is NOT a city, town, or incorporated area that has a population of greater than 20,000 inhabitants (1st Interpretation)*
    - *Any area that is NOT any urbanized area contiguous and adjacent to a city or town that has a population of greater than 50,000 inhabitants (1st Interpretation)*

Consultation Q&A (cont'd)

- Will there be geographic/regional/state differences in the design and service offering? Who will decide the differences?

- What approach will FirstNet take in building the Network? Will it be a phased approach or "big bang"? Will it be a State-by-State approach? Will it be prioritized by public safety coverage gaps or by population density?

- Does FirstNet intend to build or buy a network?

- Please explain the differences between primary and secondary users of the network.
    - *Secondary user is any user that seeks access to or use of the NPSBN for non-public safety services (1st Interpretation)*

- When FirstNet's issues their RFP, what are FirstNet's presumed requirements for the State of Florida?

- Will FirstNet require private partners to agree to the local control requirements of the public safety community (including, for example, the ability to influence change management, system maintenance windows, priority and preemption)?

- We have concern with the RFC comment on "all or a portion" of the spectrum being dedicated to secondary usage. Please explain FirstNet's justification for using the word "all", as this is primarily a public safety network.

Consultation Q&A (cont'd)

- Aside from the core first responder disciplines, what other users do you anticipate being allowed to utilize the network?

- Without collection of usable assets and State first responder requirements, how can FirstNet issue an RFP for network solutions?

Security

- How does FirstNet envision protecting public safety data within the Network RAN(s) and Core (s)?

- Has FirstNet contemplated how to protect public safety in the event that a private sector partner or opt-out State fails to build and deploy a RAN? If so, what are those plans?

- Will FirstNet be drafting any legislation to protect the data?

Financial

- What is the final amount received from the FCC auction?
    - $44,899,451,600 *(Gross)* / $41,329,673,325 *(Net)*
- Above the $7 billion, what amount of revenue from the FCC auction will be allocated to FirstNet activities?
    - *No*
- What are the special conditions of the sale of the spectrum?

Consultation Q&A (cont'd)

- Will the State of Florida be provided an opportunity to participate in the vendor selection process for the build out of the Network?

- Has there been any indication of what private partner requirements exist to make an investment to build and operate the NPSBN?

- Can you tell us what private partners have shown an interest in the network?

FloridaNet Updates

Since June 26th Executive Committee Meeting

- 07/09/2015 EMS Meeting (Orlando, FL)
- 07/13-14/2015 CJIS Symposium (Ponte Vedra Beach, FL)
- 07/27/2015 Draft RFP Review/Comment Submission to FirstNet
- 08/2015 Contract Vehicle Survey White Paper Complete
- 08/13/2015 FirstNet/FloridaNet presentation to Governor Scott
- 08/14/2015 Budget Meeting (Informal)
- 08/15-19/2015 APCO (Washington, DC)
- 08/22/2015 Revised Budget Submitted
- 08/25/2015 Organizational changes—Rhonda Mackinnon (Project Coordinator)
- 08/28/2015 FloridaNet Technical Committee Meeting (Online)
- 09/2015 Contract Vehicle Survey Complete, Data Collection Efforts Began
- 09/29/2015 Attended/presented at Police Department Communications Summit (Orlando, FL)
- 09/30/2015 Collected data submitted to FirstNet
- 10/07-09/2015 Attended 2nd SPOC meeting (Westminster, CO)
- 10/16/2015 Cybersecurity Review/Comment Submission to FirstNet
- 11/17-18/2015 Attended APCO (Atlanta, GA)
- 11/18/2015 Attended RDSTF Region 7 Workgroup

Draft RFP Response

Florida responded to FirstNet's Draft RFP on July 27, 2015. The RFP solicited 647 comments on their functions of the Operational Architecture. Florida responded to 51 pertinent areas of the Architecture.

For a majority of the responses, Florida stated that the responsibility should go to Public Safety, FirstNet and the Contractor. FirstNet should establish the architecture through direct state consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and polices. This pertained to:

- Priority & QoS Administration
- Profile Configuration Setup
- Implementing Profile Changes
- Development of Local Control User Operations Guideline
- Operations Guideline for Static & Dynamic Profiles
- System Hardening Design
- Security Policy Enforcement
- Defining, Implementing & Monitoring Network Policies & Procedures
- Defining Standard Policies for User Profiles
- Static QPP Profile Definition
- User Subscription Profile Definition
- Dynamic QPP Profile Definition
- QPP Administration
- Management and Enablement of Dynamic User Profiles
- Management of Access Class Barring
- Management of QCI
- Immediate Peril Service
- ARP Management
- Real Time Priority & Role based QoS Execution
- Processing of Responder Emergency Invocation
- Implementation of immediate Location & Priority
- Management and Enablement of Static User Profiles

For other items , the responsibility fell upon FirstNet and the Contractor. This pertained to:

- Public Safety ICS Training
- Device Administration of Secondary User via CLA
- National Network Operations Center Management
- Intrusion Prevention and Recovery
- Internal/External Security Compromise Detection

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Priority & QoS Administration	A.3.3	The administration of all priority and QoS policy frameworks for the NPSBN.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Profile Configuration Setup	A.3.3.1	Setup and configure parameters of user QoS and priority profiles for different services and applications in the NPSBN.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Implement Profile Changes	A.3.3.2	During an incident and periods of heavy NPSBN congestion, the priority and QoS configured in the default QoS profiles needed to be updated to allow emergency responders to have priority to obtain the communication services and resources to save lives.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Development of Local Control User Operations Guideline	A.3.4.2.1.2	Develops guideline to support network monitoring, provisioning, QPP provisioning, and accounting.		White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	Public Safety should develop the operational aspects of local control as it relates to public safety missions. The contractor(s) and FirstNet should develop the technical operational guideline for how local control may function. A network monitoring system should provide a mechanism for local users to report issues up to FirstNet and the contractor, along with FirstNet and the contractor's ability to report issues down to the local users.
Operations Guideline for Static & Dynamic Profiles	A.3.4.2.1.2.1	Develop and manage the operational guideline for static and dynamic profiles implementation, management and change control within the local agency to support their implementation of user's roles under QPP and its priority.		White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	These guidelines should be developed by public safety, contractor(s), and FirstNet. The management of these profiles should be maintained by public safety.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
System Hardening Design	A.3.4.2.8	The NPSBN must meet reliability metrics (reference SLA sections). The overall System Hardening Design includes development of the necessary costs and detailed Bill of Materials for geographic threat-based RAN and core hardening to meet availability SLAs. The awardee(s) will implement System Hardening on elements as agreed.		White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	The SLA's metrics and design of system hardening should be created by FirstNet, contractor(s), and States' Public Safety Entities through direct State consultations. Additionally, some States, such as Florida, already have specific hardening standards for hazards specific to the State that should be followed.
Disaster Recovery Planning/Design	A.3.4.2.8.3	Develops the mobile/deployable architecture, equipment planning (including sizing and staging locations), overall Concept of Operations (CONOPs), and organizational support structure to maintain appropriate reliability measures during disaster scenarios.		White - Comments Solicited	ORANGE	Public Safety and Contractor	Public Safety in Florida already operates a similar function. This function is owned by the Division of Emergency Management under the Emergency Support Function 2 (Communications). The contractor should work with DEM's (ESF-2) to ensure the contractor owned deployables are staged in appropriate locations. The contractor should also maintain the reliability measures and provide an after action report detailing the reliability of the network in disaster scenarios.
Opt Out State Billing Administration	A.3.5.2.4	Provide systems capability and services to administer user billing for primary and secondary users in opt-out states. Maintain detailed records of CDRs and other billing records for historical review.		White - Comments Solicited	GREEN		This should be determined during the opt-out negotiations, which will be in the best interest of public safety users to include most subscribers.
Network Events & Alerting Administration	A.3.7.5.1	Reporting of network outages or errors for alerting network engineers to address immediately. Severity levels of incident can be created based on network impact.		White - Comments Solicited	YELLOW		These outages or errors should communicated real-time and also be supplied directly to affected public safety users. A network monitoring system should provide a mechanism for local users to report issues up to FirstNet and the contractor, along with FirstNet and the contractor's ability to report issues down to the local users.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Public Safety ICS Training	A.3.8.2.1.1	Development of network training programs to support of ICS communications staff for incident and event communication management.		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	After developing these training programs, FirstNet and contractor(s) should administer them. Without actually administering these programs, the staff will not know how to operate. If any of the future funding of this training is in the form of a grant, FirstNet and contractor(s) must work through the State Administrative Agency, which is the Florida Division of Emergency Management in the State of Florida.
NPSBN feature demonstrations	A.3.8.2.1.2	Demonstrate and showcase FirstNet-specific features and functionality for FirstNet stakeholders and agencies including QPP, PTT, location, LMR/LTE interconnectivity, device range and RF performance.		White - Comments Solicited	YELLOW		After demonstrating and showcasing, contractor(s) should allow public safety to field test the features and functionality to provide feedback.
Network Configuration Management	A.3.8.2.3.1	Manage the configuration of all NPSBN equipment for network operations to ensure design and operational compliance. All NPSBN nodes need to be configured to meet design and service requirements that meet the public safety needs.	Q-OPS-4	White - Comments Solicited	YELLOW		The contractor(s) must perform this function as designed in the approved State Plan, which should be developed through direct State consultation.
Problem Management	A.3.8.2.3.6	Problem management entails the identification of network or service fault or performance degradation and taking the steps necessary to isolate and resolve the trouble incident. This can also include establishing a temporary fix of the problem to restore service until the a permanent fix can be implemented.		White - Comments Solicited	YELLOW		This process should be determined in the SLA. The contractor(s) should also immediately report any identified service fault or performance degradation to affected public safety entities.
User Equipment Certification	A.3.8.2.4.1.4	Provide appropriate test suites to ensure that devices authorized and certified as FirstNet compliant work in the desired manner. Support appropriate network specific tests, such as RAN IOT and vertical features specific to FirstNet.		White - Comments Solicited	GREEN		FirstNet should utilize an independent lab, such as those found at the Public Safety Communications Research (PSCR) Lab.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Device Administration of Secondary User via CLA	A.3.8.2.4.1.5	Devices used by secondary users may not conform to the entire FirstNet testing suite. This function manages the types and nature of secondary user devices allowed to access the network (e.g., M2M modems).		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	The contractor(s) involved in the CLA and RAN arrangements should manage the types of secondary user devices, while FirstNet manages the nature of secondary devices. It is imperative that when public safety needs priority and preemption capabilities, that no secondary equipment interferes with those features.
Interconnection Testing	A.3.8.2.4.3	Testing of interconnection services, especially those connecting between eNB and the FirstNet core for both opt-in and opt-out states. Security testing of these links may also be incorporated.	Q-RC-19, 21	White - Comments Solicited	GREEN		Security testing of these links must be incorporated.
Service Availability Management	A.3.8.2.4.6.2	Availability management ensures that systems are sized and architected to meet the Service Level Agreements. This includes ensuring proper contingency plans are in place and tested as well as continually reviewing architecture needs in terms of redundancy and high availability based on business needs.		White - Comments Solicited	YELLOW		The contractor(s) must perform this function as designed in the approved State Plan, which should be developed through State consultation. Additionally, the "continually reviewing architecture needs" should be on a schedule determined in the State Plan.
Service Capacity Management	A.3.8.2.4.6.3	Capacity management ensures that services are architected with the capacity to meet current and immediate future business capacity needs.		White - Comments Solicited	YELLOW		This function's description should be amended to incorporate long-term capacity needs. The contractor(s) should revisit this function on an basis agreed in the State Plan in order to maintain needed public safety capacity requirements.
Service Level Management	A.3.8.2.4.6.4	Service level management is the identification and monitoring of relevant KPIs to ensure end user quality of service metrics are met or exceeded.		White - Comments Solicited	GREEN		FirstNet should identify and monitor KPIs as designed in the approved State Plan, which should be developed through State consultation.
Security Policy Enforcement	A.3.8.2.5.4	Provides Governance on security policy and also policy and procedures related to security threats, mitigation, logging and enforcement capability. FirstNet, Agency and the contractor(s) shall provide the procedure, process for Security Policy enforcement.		White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	Local users should also have access to monitoring security threats. This is especially important due to the CIJS logging requirements.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Disaster response information gathering	A.3.8.2.6.2	The contractor(s) will support intelligence gathering to understand the specifics of each DR or major event. Information gathered will include event location, scope (geographic and capacity), environmental and access issues, deployment considerations (for example backhaul, power), and estimated event duration.		White - Comments Solicited	YELLOW		This function should be performed utilizing methods currently in place for commercial networks. This information should also be shared with affected public safety entities.
Agency Coordination	A.3.8.2.6.3	Once a disaster event occurs or a major event is planned, the contractor(s) will coordinate deployment of assets and support staff with the lead agency(ies) that require support. The lead agency(ies) may be at the local, state, or federal level.		White - Comments Solicited	YELLOW		FirstNet should develop the definition of "lead agency" through direct State consultation. Regardless of the "lead agency", the policies determined by the State in the consultation process should be followed.
Event Tracking	A.3.8.2.6.4	Disaster Response or major event support will be tracked by the contractor(s) allowing coordination of staff and assets, documentation of support costs, and after action reporting.		White - Comments Solicited	YELLOW		The after action report should be completed in a timely manner and supplied to public safety and FirstNet immediately after it is completed.
Mitigation Plan Development	A.3.8.2.6.6	Develop plans to deploy mobile assets in a timely manor to restore public safety communications in affected areas. Such items include fuel limitations, damaged access, equipment failure, and backhaul/transport impairments. Plans will be continuously updated based on after action reporting.		White - Comments Solicited	ORANGE	Public Safety and Contractor	These plans should be developed in coordination between public safety and the contractor. The contractor should have the responsibility of carrying out the plans. Additionally, the after action reporting should be conducted in a timely manner and supplied to public safety and FirstNet immediately after completion.
Post Incident & Event Analysis Reporting	A.3.8.2.6.7	Post incident/event analysis reporting of major events and disaster scenarios for incorporation into process modifications and training programs to drive and realize continuous improvement for future disaster recovery and major events.	Q-OPS-21	White - Comments Solicited	YELLOW		Contractor(s) should provide these reports to affected public safety users immediately.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
National Network Operations Center Management	A.3.8.3.1	The Nation Network Operations Center provides and manages nationwide network monitoring visibility to proactively and reactively resolve issues that may impact user services. The National Network Operations Center serves as the coordination point (managing tier 2-3 teams) to optimize service restoration.		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	This National NOC should report any pertinent information to the State NOC in real-time. The definition of "pertinent information" should be determined through direct State consultation and detailed in the State Plan.
Agency Security Operations Center Management	A.3.8.3.2	The contractor(s) will establish protocols working with FirstNet and Agency SOC's to ensure agency applications and data remain secure.		Green - FirstNet Only	GREEN		FirstNet should establish these protocols through direct State consultation.
Intrusion Prevention	A.3.8.3.2.1	Prevent security intrusions by proactive and real-time sampling of network traffic and reviewing logs to detect and eliminate in-progress and future threats.		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	The contractor(s) must perform this function with oversight from FirstNet. Any security issues should be reported to public safety in real-time.
Intrusion Recovery	A.3.8.3.2.2	Recovery from security intrusions by proactively removing malware or other security threats from the NPSBN and documenting how the intrusion occurred and steps required to prevent reoccurrence.		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	The contractor(s) must perform this function with oversight from FirstNet. Any security issues should be reported to public safety.
Internal Security Compromise Detection	A.3.8.3.2.3	Detecting threats originating from within the trusted network or system.		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	The contractor(s) must perform this function with oversight from FirstNet. Any security issues should be reported to public safety. Internal intrusions should be reported to the originating agency so security measures can be implemented.
External Security Intrusion Detection	A.3.8.3.2.4	Detecting threats originating from outside the trusted network.		White - Comments Solicited	ORANGE	FirstNet and contractor(s)	The contractor(s) must perform this function with oversight from FirstNet. Any security issues should be reported to public safety.
NPSBN Security Operations Center Management	A.3.8.3.4	Monitoring, detecting, and resolving incidents that may affect the confidentiality, integrity, or availability of network devices, end-user devices, and systems.	Q-OPS-12	Green - FirstNet Only	GREEN		Monitoring should be 24/7/365 with any identified issues being reported to public safety in real time.
NPSBN Security Intrusion Monitoring & Detection by SOC	A.3.8.3.4.1	Surveillance and identification that an unauthorized access attempt has been made, is occurring, or has occurred.		Green - FirstNet Only	GREEN		Monitoring should be 24/7/365 with any identified issues being reported to public safety in real time.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Define, Implement, & Monitor Network Policies & Procedures	A.4.2	Develop, implement, and monitor overall operating policies and procedures for the NPSBN fully compliant with all laws, rules, standards, and regulations, applicable to FirstNet.		White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	Public Safety should develop the operating policies. Contractor(s) should implement the operating policies. FirstNet should monitor the operating policies.
Define & Implement Operational Procedures	A.4.2.1	Define operational procedures to be implemented throughout NPSBN. These operational procedures would provide guidance to field teams on the optimal methods to ensure network performance meets all NPSBN requirements.		White - Comments Solicited	ORANGE	Public Safety and contractor(s)	Public Safety should develop the operating policies. Contractor(s) should implement the operating policies.
Define Standard Policies for User Profiles	A.4.3	Develop the user policy profile framework which includes static, dynamic, and subscription profiles.	Q-DEV-1, Q-RC-2	Green - FirstNet Only	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Static QPP Profile Definition	A.4.3.1	Develop the user policy profile framework specifically for static, non-emergency situations.	Q-RC-2	Green - FirstNet Only	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
User Subscription Profile Definition	A.4.3.2	Define all user subscription profiles for NPSBN services such as voice, data, push-to-talk.	Q-DEV-1, Q-RC-2	Green - FirstNet Only	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Dynamic QPP Profile Definition	A.4.3.3	Develop the user policy profile framework specifically for dynamic, emergency situations.	Q-RC-2	Green - FirstNet Only	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Implement & Enforce Policy Procedures Across Agencies	A.4.10	Implement and enforce FirstNet security policies, business processes, and operational procedures within the local agencies.		Blue - Public Safety	BLUE		These policies, processes, and procedures should be developed through direct State consultation and agreed upon in the State Plan development process.
Agency Administration Program Support	A.5.1	Responsible for coordinating with state, federal, tribal, or other agencies for any agency-specific program needs or reporting.		White - Comments Solicited	YELLOW		Agency-specific needs must not interfere with the greater functioning of the network.
QoS, Priority, and Preemption (QPP) Administration	A.7.1.6	Defines, plans, obtains the acceptance for the QoS, Priority, and Pre-emption mechanisms. Centralized authorization, identity management, and subscriber information and QoS, Priority, and Pre-emption policies would be employed to manage the distribution of control across the agency/FirstNet touch points.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Management and Enablement of Dynamic User Profiles	A.7.1.6.1	Dynamic Incident Management allows QPP administration capable of performing real time changes to application and user profiles, leading to QCI, ARP and Access Class barring changes, in the course of an incident and returning the public safety users to their pre-incident levels following the completion of the incident.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Management of Access Class Barring	A.7.1.6.1.1	Access Class Barring includes the implementation of a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2 within QPP administration.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Management of QoS Class Identifiers (QCI)	A.7.1.6.1.2	Enable and support of all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Immediate Peril Service Management	A.7.1.6.1.3	This network services allows for the immediate raising of priority for first responders who activates his or her immediate peril button. Public safety will define the order of services and their priority following the invocation of immediate peril and QPP administration application function must be capable of executing this in real-time and returning the public safety user to its pre-immediate peril profile following the clearing of this state. The service will provide immediate location of the first responder(s) who active their immediate peril button(s)	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Allocation and Retention Policy (ARP) Management	A.7.1.6.1.4	This network service defines support for the usage of all 15 ARP values defined in 3GPP and ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203 within QoS, Priority, Pre-emption administration.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Real Time Priority & Role based QoS Execution	A.7.1.6.1.5.1	This network service provides administration of real time priority and role based QoS changes (leading to QCI, ARP and/or Access Class barring changes) in the course of an incident and returning the public safety users to their pre-incident levels following the completion of the incident.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
Processing of Responder Emergency Invocation	A.7.1.6.1.6	This network services supports the immediate raising of priority for a first responder who activates his or her responder emergency button. Public safety will define the order of services and their priority following the invocation of responder emergency and QPP administration application function must be capable of executing this in real-time and returning the public safety user to its pre-responder emergency profile following the clearing of this state.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Implementation of Immediate Location & Priority	A.7.1.6.1.6.1	This service allows for the immediate raising of priority for first responders who activates his or her responder emergency button and the immediate emergency location request of the public safety user by the network. Public safety will define the order of services and their priority following the invocation of responder emergency and immediate location. The QPP application and location function must be capable of executing these requirements in real-time and returning the public safety user to its pre-responder emergency profile following the clearing of this state.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.
Management and Enablement of Static User Profiles	A.7.1.6.2	Create and manage QPP profiles that include a user's static QPP configuration (including QCI, ARP, QBR, GBR, APN-AMBER, and UE-AMBER) to meet FirstNet's first responder needs. These needs include users being able to communicate and access PS applications during incidents.	Q-RC-2	White - Comments Solicited	ORANGE	Public Safety, FirstNet, and Contractor	FirstNet should establish the architecture through direct State consultation. Public Safety should develop the policy as it relates to the local public safety mission. Contractor(s) should develop the technical capabilities to ensure the implementation of the architecture and policies.

Cybersecurity Notice—FL

Comments were submitted to FirstNet on October 16, 2015.

Florida was concerned with the following items:

- **Fraud Prevention and Revenue Assurance**
    - *FirstNet should factor in that current users maintain an "unlimited data plan" and would want that as an option*
    - *It is imperative that charging and service controls are used to ensure end-to-end QoS for public safety and should not be compromised in order to monetize the system*
- **Heterogeneous Networks**
    - *Any "third-party" hardware and software must be tested to ensure confidentiality, integrity, and availability (CIA)*
    - *If public safety is off-loaded to WiFi networks, the Offeror must maintain the same CIA, and should not be billed the same*
- **Training**
    - *Offeror will directly, or via government subsidies, train Public Safety users of the network*
    - *Consistent training throughout the nation, and continuously*
- **Devices should be continuously monitored**
    - *Request definition of "offline"*
- **Bring Your Own Stuff**
    - *Offeror needs to work with agencies regarding on the policies when using their "stuff"*
- **Application Security Certification**
    - *Minimum standards to be applied should be included*
- **Data Loss Prevention**
    - *The section addresses protection and not prevention and needs to add prevention activities*
- **Identity Assurance**
    - *Should include ways to identify each user when multiple users are sharing a single device simultaneously*
- **Risks**
    - *Florida requests further clarification on risk acceptance and viability of mitigation*
    - *Need to weigh Public Safety risk at an appropriate level agreed upon in the State Plan*
    - *Who will be responsible for evaluating and ranking identified risks, as well as the controls?*
    - *Who will be responsible for procuring the insurance against risk?*
- **Communicate**

    - *Should include using existing information-sharing infrastructure*
- **User Configuration and Visibility of Security**
    - *Include language regarding current notification best practices*
- **Federal Bureau of Investigation's (FBI) CJIS Security Policy**
    - *The network must not be precluded from other functions due to stringent and bureaucratic requirements*
- **Scheduled cyber security exercises**
    - *Need to update "as needed" to continuous, predetermined and agreed upon timetable*
- **Engineering a Resilient Network**
    - *Requests clarification of the definition of "economically reasonable", and the State should assist in this*
- **Security incidents and after action reports**
    - *Include language regarding information sharing between the Offeror, FirstNet and the States*
    - *Need a defined timeframe and protocol for incidents to be disclosed*
- **Monitoring, Information Sharing and Collaboration**
    - *Include language regarding direct information sharing with the State, with a defined timeframe and protocol for disclosure*
- **Independent Applications/Services Testing**
    - *State needs to aid in the definition of "reasonable assurance" of security*
- **Alternative methods, such as VPN, are critical**
    - *Need definition of "practical" and the Offeror needs to supply a best practice solution alternative*
- **Security Information and Event Management**
    - *Request FirstNet to update the language to include information sharing to States through existing information-sharing infrastructure*
- **Network disparately deployed can become cost-prohibitive rapidly**
    - *Hardening should be provided to every State and FirstNet and the States should agree upon hardening requirements*
- **Retention of any data will be in accordance with agency record retention policy**
    - *Add language regarding the physical destruction and/or hard drive wiping requirements*

Cyber Security Comments Template

Item	Page No.	Paragraph Ref/Sentence	Question/Comment	Government Response	RFP Change
1	6	2.2e. 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.	The State of Florida agrees that the NPSBN should have a fraud protection functionality to ensure those that are authorized to utilize the network and the Priority and Preemption Quality of Service receive these functionalities without interference from unauthorized users. The State, however, points out that many potential NPSBN users currently maintain an "unlimited data plan", which FirstNet should consider in order to promote user adoption. Additionally, the State believes it is imperative that charging and service controls are used to ensure end-to-end QoS for Public Safety rather than as a mechanism to attempt to reduce the data rate of Public Safety in order to "appropriately" monetize the excess capacity being used by secondary users.		
2	6	2.2j. 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.	The State of Florida agrees that the network should enable small cells and heterogeneous networks to securely authenticate to and interconnect to the core network. Such a situation will allow for greater coverage indoors, for example, or reduce NPSBN congestion through WiFi-off-loading. The State comments that any "third party" hardware and software must be tested to ensure confidentiality, integrity, and availability. The State also notes that if Public Safety users are off-loaded to WiFi networks, the Offeror must maintain the same data confidentiality, integrity, and availability through appropriate protections. Additionally, if Public Safety users are off-loaded to WiFi, such data transmissions should not be billed in the same		

			manner as those transmissions utilizing the NPSBN resources.		
3	8	2.2v. 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 key methods to increase the cyber security of the NPSBN.	The State of Florida agrees that training the potential Public Safety users will be one of the most important factors in maintaining the security of data. The State believes that the Offeror will either directly, or via government subsidies, train all Public Safety users of the network. Additionally, the training should be consistent across the Nation, and provided on a continuous basis. Benchmarks will also help establish effectiveness of training materials (ex: a Phishing test to trainees).		
4	8	2.2. 3.a.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.	The State of Florida requests a definition of "offline".		
5	9	2.2 3.g. Bring Your Own Stuff – Cyber security solutions should address "Bring Your Own (Device, Application, or Wearable)."	The State of Florida agrees that the Offeror's cyber security solution should address "Bring Your Own Stuff" as there are many smaller and voluntary agencies operating across the State that do not have the resources to purchase "agency-owned devices". The State maintains that the Offeror should work with individual agencies on policies regarding the data on the "stuff" (such as the need to wipe all organizational and personal data from a lost/stolen personal device being used for Public Safety operations).		
6	10	2.2 4.e. Application Security Certification –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.	The State of Florida agrees that all applications operating on the network undergo a defined certification process. The State believes this should go one step further to include minimum standards to be applied.		
7	11	2.2 4.l. Data Loss Prevention – The solution should provide protections to ensure applications protect data while at rest, in use, and in transit.	The State of Florida agrees that the solution should provide protections. This section is labeled as "Data Loss Prevention", but does not address prevention, rather this section solely focuses on		

			protection. The State believes that FirstNet should revise this section to include language related to prevention activities, while maintaining the protection clause.		
8	11	2.2. 5.b.i. Identity Assurance – The solution should ensure the following relationships are always authenticated:	The State of Florida agrees that authentication will be required to maintain cyber security. The State requests that FirstNet include a suggestion that relates to identifying each user when multiple users are sharing a single device simultaneously. For example, a shared mobile terminal in a Fire Engine, or multiple firefighters on a single mobile data computer.		
9	12	2.3 5.b-d. 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.	The State of Florida requests further clarification on risk acceptance and viability of mitigation. The State believes it is imperative for FirstNet to weigh Public Safety risk at an appropriate level agreed upon in the State Plan. The State also requests clarification as to who shall be responsible for evaluating and ranking identified risks, as well as devising and implementing subsequent controls. The State would also request clarification as to who will be responsible for procuring the referenced insurance against risk and what the mandated insurance limits will need to be.		
10	13	2.4 1.e. Communicate among internal and external stakeholders about cyber security risk.	The State of Florida agrees that cyber security risk must be shared. The State suggests including language regarding the synergistic benefits of utilizing existing information-sharing infrastructure, such as the Fusion Centers operating across the Nation.		
11	13	2.4 2.e User Configuration and Visibility of Security – Provide an opportunity for the user to check if the security features are in operation	The State of Florida agrees that the Offeror should provide an indication of security features. The State suggests that FirstNet include language regarding current notification best practices, such as a visible icon. This may help reduce confusion and increase efficiency since a user will not have to search for an indication of security.		

12	14	2.4 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].	The State of Florida maintains that the network shall be CIJS and HIPPA compliant. The State notes, however, that the network must not be precluded from other functions due to stringent and bureaucratic requirements.		
13	15	2.5 6.d. Runs large-scale scheduled cyber security exercises and targeted local cyber security exercises as needed.	The State of Florida requests FirstNet to update the language of this clause from "as needed" to a continuous, predetermined and agreed upon timetable.		
14	15	2.5 7.a, c Engineering a Resilient Network. This requires balancing single-points-of-failure and economics. In short, it is about understanding and managing risk. FirstNet's network architecture, which will ensure that single points of failure are reduced as low as economically reasonable.	The State of Florida understands that there will be a finite amount of economic resources. The network must meet the intent of the Middle Class Tax Relief and Job Creation Act of 2012, though. Therefore, the State requests clarification of the definition of "economically reasonable". Additionally, the State believes it is the intent of the Act, through required State consultation, that the State aid in the definition of "economically reasonable".		
15	16	2.7 1.i-k. 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.	The State of Florida requests that FirstNet include language regarding information sharing between the Offeror, FirstNet, *and* the States in all of the clauses listed. The State also requests a defined timeframe for incidents to be disclosed to the State, as well as the protocol to be enacted for conveyance of the disclosure.		
16	16, 17	2.7 2.b, e, h. b. 24/7/365 cyber security monitoring of core infrastructure e. Establishment of the baseline network activity and utilization to use as a reference	The State of Florida believes it is imperative for Public Safety users to be knowledgeable of any network intrusions in order to maintain the highest level of cyber security. Therefore, the State requests that language be included regarding direct information sharing to each State. The State also		

		h. Information Sharing and Collaboration that integrates and disseminates information throughout the critical infrastructure partnership network. Processing and posting Suspicious Activity Reports. 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. 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.	requests a defined timeframe for incidents to be disclosed to the State, as well as the protocol to be enacted for conveyance of the disclosure.		
17	18	2.9 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.	The State of Florida agrees that testing, validation, and authentication are necessary to maintain data confidentiality, integrity, and availability. The State maintains that consistent to the Act, through required State consultation, that the State aid in the definition of "reasonable assurance" of security.		
18	18	2.10 1.a. If this is not practical, then alternative methods, such as VPN, are critical.	The State of Florida requests a definition of "practical". Additionally, if an "out of band network" is not "reasonable", then the Offeror shall supply a best practice solution to Public Safety users, as agreed upon in the State Plan.		
19	19	2.10 5a. 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	The State of Florida agrees that a SIEM tool will be necessary to maintain security. While the State understands that the information gathered may be too technical for a majority of end users, the Offeror could create a high-level mapping tool which shows, in colors (such as green, yellow, and red), the status of the network. Additionally, the State requests FirstNet to update the language of		

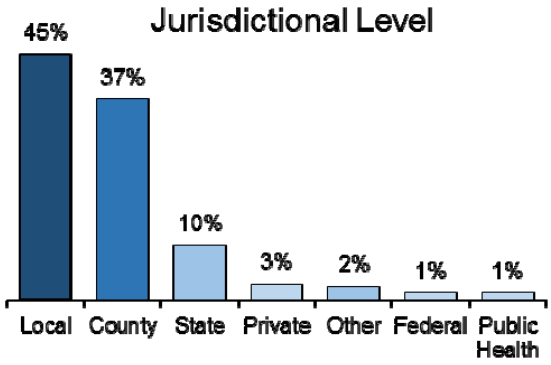
		and switches, and servers. The SIEM is responsible for the aggregation and normalization of security-related data and allows for analysis on a large number of logs in an efficient manner.	this clause to include information sharing directly to States through Fusion Centers, Network Operation Centers, or some other existing information sharing infrastructure.		
20	20	2.11 1. However, because the FirstNet wireless network will be disparately deployed across the nation, this can become cost-prohibitive rapidly.	The State of Florida believes this sentence is inappropriate and does not meet the intent of the Act. The State understands that each State may have their own set of potential risks and threats. This does not mean that hardening should not be provided to every State, however. The State also understands that physical security and hardening will be too expensive to provide to every cell site. Therefore, the State maintains that FirstNet, acting through the required State consultation, provide specific and agreed upon hardening requirements for the State Plan.		
21	20	2.12 4-5. 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.	The State of Florida agrees that local data retention policies, along with Federal policies, must be followed in this network. The State requests language regarding the physical destruction and/or hard drive wiping requirements to be added to this appendix.		

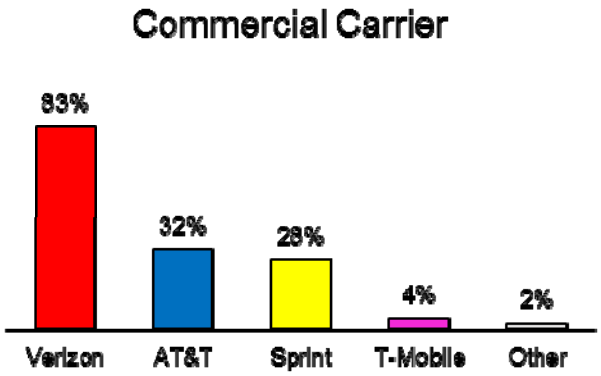
Contract Vehicle Survey

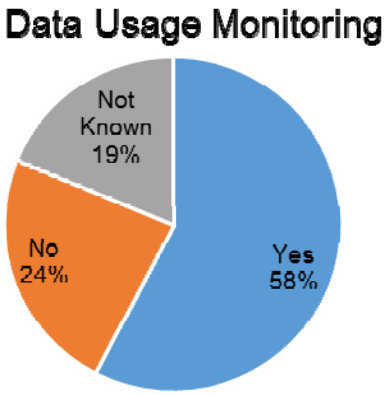
Overview

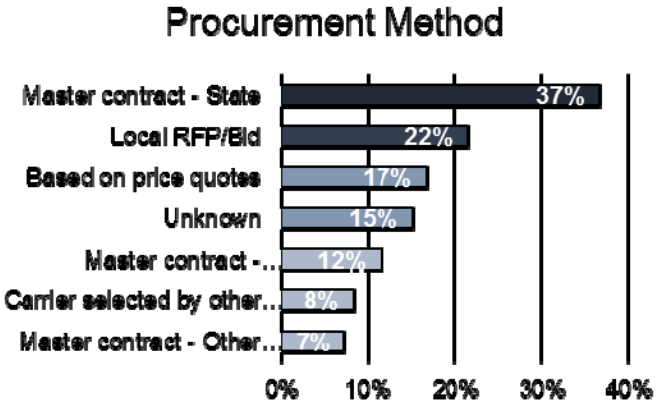
- Conducted survey from January to September
- Aggregated survey info and sent to FirstNet
- Produced white paper with the following highlights

Highlights









Contract Vehicle Survey

White Paper

August 2015

This document is an abbreviated version of the original document. It has been reduced to just include the Executive Summary, the Introduction and the Conclusion. To review the complete document, please visit: www.floridanet.gov/documents.

Learn more at FloridaNet.gov

Contact Us at FloridaNet@flhsmv.gov

Follow Us at twitter.com/FLFirstNet

Like Us at facebook.com/FloridaNet

This document was prepared by FloridaNet using funds under award 12-10-S13012 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC, or FirstNet.

Executive Summary

The Contract Vehicle Survey was modeled after a Federal survey created specifically for the National Public Safety Broadband Network initiative. The FloridaNet team utilized this as a starting point to ensure critical data were being provided to FirstNet. The Federal survey, in its native form, was quite lengthy. Therefore, the FloridaNet survey was shortened to 18 of the most pertinent questions. This approach was utilized in order to encourage participation and reduce respondent fatigue.

FloridaNet derived a contact list through various methods and external aid. The survey was formally open for one month, with Region 5 acting as a testing beta. Six hundred sixty six of the thousands of public safety entities identified received a direct invitation to participate in the survey. This sampling error resulted from the lack of a comprehensive contact list, but did not appear to skew further interpretations of the data. The final compiled data suggest that a relatively representative sample of the State's target population did fully complete the survey.

The survey was completed by 250 public safety professionals from 53 counties across the State of Florida. These respondents were from both traditional first responder professionals (Law Enforcement, Fire, and EMS), and non-traditional responders such as public utilities, health, and transportation services. Additionally, a wide range of jurisdictional levels were represented, ranging from Federal to Special Districts, with County and Local having the highest proportion of responses (37% and 45%, respectively).

The professionals were queried on three main topics: demographics, carrier information, and devices. The demographics topic provided insight regarding a respondent organization's workforce, data equipped vehicles, and data usage monitoring tools. The size of the workforce indicated that the sample was representative of the State, as small, moderate, and large organizations were represented in a manner consistent with the overall ratio found within the State (36% small, 30%, moderate, 15% large, and 19% very large). Additionally, the ratios of data equipped vehicles were commensurate with the numbers of full time employees, which may indicate validity.

The demographics topic also contained one of the most important questions for future data collection requirements: the usage of a data monitoring tool. A majority of organizations (56%) indicated that their organization does collect data usage. It is a goal of FloridaNet that these databases will be shared in the hopes of obtaining data such as application throughput requirements and response latitude/longitude locations. This

information will be then used to create a GIS map to show FirstNet what Florida's public safety users need and expect from the National Public Safety Broadband Network.

In addition to the demographics of respondents, the survey looked at current commercial offerings. The majority of respondents (86%) utilized Verizon's network and procured their carrier through the State's Master Contract (35%). The most important factors in choosing a network were coverage areas (73%) and redundancy (53%). All of these results highlight the need for a flexible procurement method and abundant coverage areas in the new dedicated network.

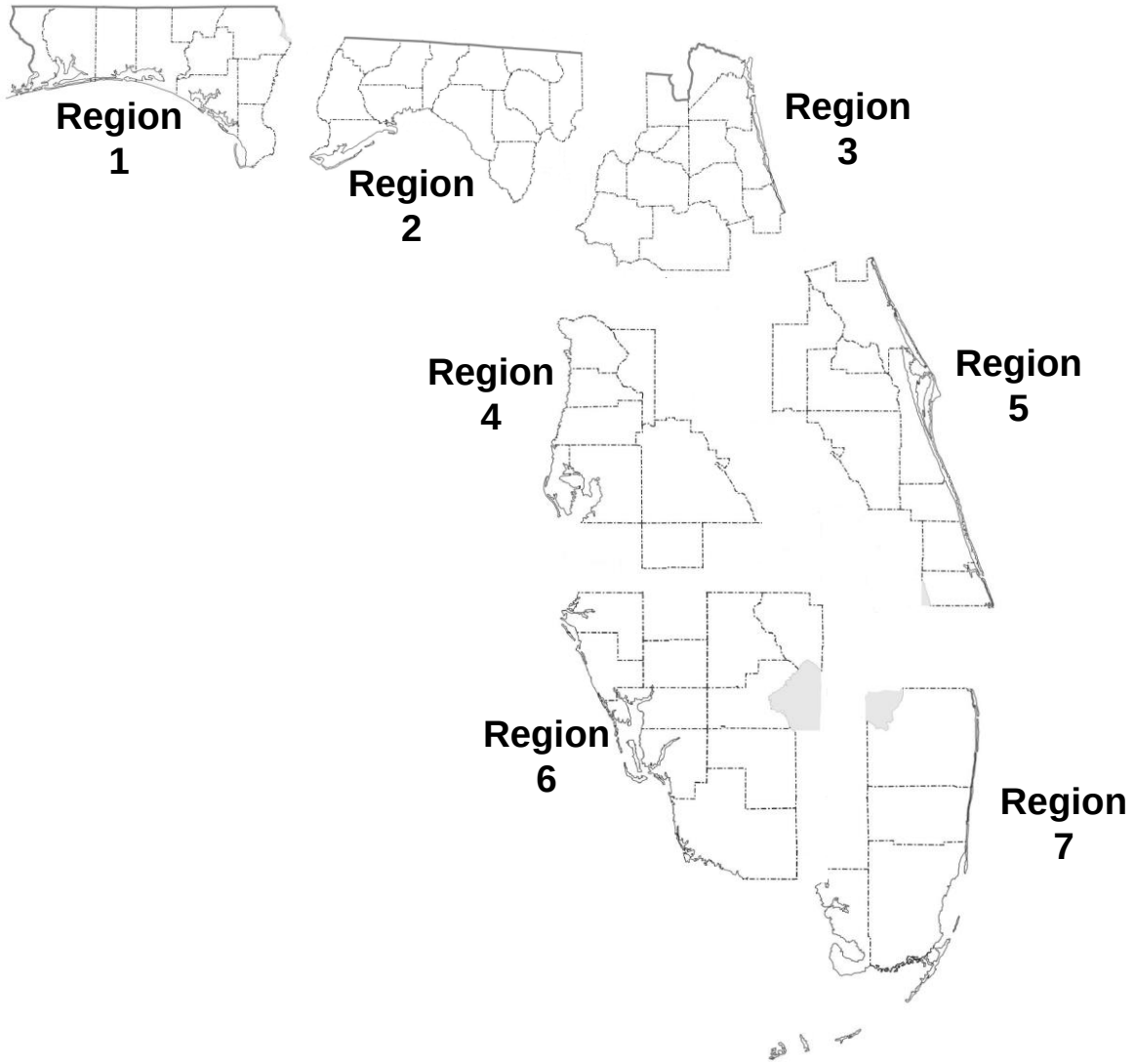
FirstNet has indicated that access to the network will cost about the same as current commercial offerings in order to obtain a high rate of public safety adoption. Rates may vary according to the type of device and the amount of data typically used by each type. The vast number of respondents maintain smart phones equipped with data and air cards, which are mobile modems that plug into devices. According to the results, a majority (80%) of potential users pay less than $50 per mobile device per month. Additionally, unlimited data plans are by far the most common form of plan (83%), regardless of the type of device.

Overall, the results from the Florida Contract Vehicle Survey are representative of the State of Florida and provide necessary insight on the potential users of this enormous initiative. Regardless of the demographic makeup of the Region, Verizon's network was the most utilized (86%) throughout the State. Additionally, a majority of respondents (83%) representing all seven regions procured an unlimited data plan. All regions, except Region 7, procured commercial data carriers through the State's Master Contract. Region 7, which has the highest population density, conducted an equal amount of Local Requests for Proposals (RFPs) as utilizations of the State's Master Contract. The more rural, and less densely populated regions monitor data usages less frequently than the urban and suburban regions.

Through the upcoming education and outreach campaigns, the FloridaNet team is determined to increase participation and awareness of all public safety disciplines. A holistic and expansive representation from across the State will ensure those that protect the lives and property of Florida residents and visitors obtain a dedicated and hardened mission critical data communications network where they need it and when they need it.

This document was prepared by FloridaNet using funds under award 12-10-S13012 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC, or FirstNet

Introduction



The Contract Vehicle Survey is a preliminary effort to gain insight on the mobile data broadband needs of Florida's Public Safety community. Specifically, this survey was aimed at understanding the potential users of the National Public Safety Broadband Network (NPSBN) as governed by the First Responder Network Authority (FirstNet). Additionally, the potential users of the NPSBN were questioned on three main topics: demographics, carrier information, and devices.

The Department of Homeland Security's (DHS) Office of Emergency Communications (OEC) Mobile Data Survey Tool (MDST) was the source of inspiration for the FloridaNet survey. This source was chosen because it is a nationwide survey that was developed

specifically for the FirstNet initiative. The MDST is very lengthy and detailed, however, which is why the FloridaNet team decided to pare down the number of questions to the 18 most pertinent. Additionally, the length of the survey was shortened in order to mitigate fatigue and encourage respondent completion.

One of the largest challenges of this survey was obtaining a list of those practitioners who would know their organization's details as they relate to mobile broadband data needs. The primary contact list used was from the DHS OEC mapping and database tool called CASM NextGen. This list, however, was not completely current, nor comprehensive. To update the list and ensure that a representative sample of public safety disciplines was developed, the Florida Department of Law Enforcement (FDLE) Regional Domestic Security Task Forces (RDSTFs) were utilized.

The RDSTFs split the State into seven regions, with two primary chairpersons for each region. The co-chairs facilitated contact with the diverse first responder disciplines throughout their respective regions and sent the FloridaNet team updated contact lists. These lists were then consolidated and verified.

Region 5 was the beta test region for the survey. The first round of survey invitations were sent on January 9, 2015. The remaining six regions received invitations on June 4, 2015. Surveys were to be completed by July 4, 2015. This was not a hard-stop, however, and the survey was open until September 15, 2015 for any public safety entity that wanted to have their voice heard. The results contained within were from August 1, 2015 or earlier.

The survey was sent to 666 practitioners across the State. Of these practitioners, 250 fully completed the survey. This represents a completion rate of 38%. It is important to note that there are thousands of public safety entities across the State. Without a complete contact list, it was impossible to reach all of these organizations. Those agencies that did receive and complete the survey represent a wide array of disciplines and demographics.

This document was prepared by FloridaNet using funds under award 12-10-S13012 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC, or FirstNet

Region 1-7

To see the results of each region's demographics, carrier information and devices, please visit www.floridanet.gov/documents to see the complete version of this document, FloridaNet Contract Vehicle Survey White Paper.

Conclusion

The goal of the Contract Vehicle Survey was to gain preliminary insights on the potential users of the NPSBN, along with their current commercial mobile data providers, the devices that are being used by Florida's public safety organizations, and what features these professionals are expecting from this nationwide initiative. The survey was completed by 250 individual practitioners from across the State representing rural, suburban, and urban demographics. Additionally, 53 of the 67 counties that make up Florida had at least one respondent, which further validates the representativeness of the diverse demographics found across the State.

The cohort with the greatest representation was from the Law Enforcement discipline, followed by Fire Services. Together, these two groups make up 58% of respondents. While this may have skewed the results from other, non-traditional, public safety respondents, the input from these two disciplines is extremely important in understanding the needs of first responders as it relates to the NPSBN. Florida has remained committed to a broad definition of "public safety" for the NPSBN. Therefore, the FloridaNet team must initiate further education and outreach to include important recovery organizations such as public utilities and health care agencies.

While there may have been underrepresentation of the non-traditional responders, there was a diverse demographic of sizes of organizations. A majority of respondents were from small to moderately sized agencies. This is consistent with the large rural swaths of Florida, where over 200 employees may not be necessary. More than half of the responding organizations utilized the help of volunteers. This fact may prove to be crucial in the establishment of protocols and procedures as it relates to bring your own device (BYOD) management.

One of the most important questions related the utilization of a data monitoring tool. Hard data will be imperative for the creation of valid coverage and capacity maps. FloridaNet hopes to gather data such as application usages, required throughput values, and responding latitude/longitude points. This information will then be consolidated and visually represented in a GIS format so FirstNet can understand what our local users need and expect out of the NPSBN.

To encourage public safety adoption of the NPSBN, FirstNet will have to meet, or exceed, current commercial offerings. A majority of respondents indicated needing only one carrier, with Verizon being the most popular across the State. Those organizations that needed two or more carriers to achieve their public safety missions did so due to required

coverage and redundancy. These results highlight the need for FirstNet to provide coverage in both urban and rural areas, while maintaining a high degree of reliability through hardening infrastructure.

The Congressionally mandated NPSBN rural milestones will also be very important for the adoption of Florida's public safety users. According to the 250 respondents, coverage was the most important factor when choosing a carrier. Additionally, the State of Florida has numerous Counties with low population densities. These counties will require the same reliable network as the densely populated ones, where commercial carriers have historically provided greater amounts of capacity and coverage. Therefore, FirstNet must provide adequate, and expanded, coverage beginning in the first phase of the NPSBN rollout.

The cost of FirstNet's data plans will also be important for high rates of adoption. According to the survey results, a majority of agencies allocate multiple data capable devices to each employee. Additionally, most respondents indicated that their organizations pay less than $50 per device per month for these services. The respondents mainly used the State's Master Contract or a Local RFP/Bid process to procure their mobile data carriers. This may show FirstNet that public safety users should have flexible purchasing options in order to encourage participation.

Finally, the survey showed promising results regarding awareness of the FloridaNet program. A large majority of respondents were at least somewhat aware of this initiative. Although this project has existed for about two years, there were not many tangible developments until the second quarter of 2015. Since this time, FirstNet has issued two requests for public comment and a draft request for proposal. These items have been thoroughly analyzed and responded to by the FloridaNet team and governance bodies. Additionally, many governance, technical, and operational aspects of the NPSBN have been developed through these documents. With these new insights, the FloridaNet team will create updated education and outreach materials to inform local public safety entities of this initiative. Local meetings will also be held in order to increase awareness of potential users.

It is a goal of FloridaNet to have the thousands of public safety users operating across Florida to become fully aware of the importance of the NPSBN. A dedicated data communications network will provide first responders, from all disciplines, with a mission critical data pathway to support their current mission critical voice networks. Additionally, the inherent interoperability of the network will ensure that aid from across the nation will be able to perform missions in conjunction with Florida's public safety organizations in the event of a major natural or manmade disaster.

	Surveys Sent	Response Rate	Number of Counties Represented	Highest Population	Lowest Population	Average Population Density	Most Common Carrier	Most Common Procurement Method	Number of Devices per Employee	Percentage of Organizations Monitoring Data	Percentage of Organizations Requiring Multiple Carriers	Price per Device per Month	Most Common Data Plan	Most Common Mission Critical Application
Region 1	45	44%	5 of 10	305,817 (Escambia)	14,625 (Calhoun)	157	Verizon (85%)	Master Contract – State (35%)	2 (55%)	45%	15%	$50 or Less (73%)	Unlimited (80%)	Internet Browsing (79%)
Region 2	76	22%	8 of 13	275,487 (Leon)	8,365 (Liberty)	67	Verizon (100%)	Master Contract – State (41%)	2 (44%)	41%	24%	$50 or Less (81%)	Unlimited (89%)	One-way Messaging (63%)
Region 3	70	46%	11 of 13	885,855 (Duval)	15,535 (Union)	228	Verizon (81%)	Master Contract – State (35%)	2 (31%)	59%	21%	$50 or Less (74%)	Unlimited (82%)	One-way Messaging (74%)
Region 4	110	23%	7 of 8	1,291,578 (Hillsborough)	27,731 (Hardee)	838	Verizon (92%)	Master Contract – State (28%)	2 (52%)	52%	28%	$50 or Less (91%)	Unlimited (83%)	Internet Browsing (84%)
Region 5	192	58%	9 of 9	1,253,001 (Orange)	141,994 (Indian River)	573	Verizon (75%)	Master Contract – State (28%)	2 (35%)	57%	51%	$50 or Less (76%)	Unlimited (79%)	One-way Messaging (79%)
Region 6	79	36%	9 of 10	661,115 (Lee)	12,884 (Glades)	253	Verizon (85%)	Master Contract – State (39%)	2 (36%)	55%	15%	$50 or Less (87%)	Unlimited (90%)	Internet Browsing & One-way Messaging (78% each)
Region 7	94	34%	4 of 4	2,662,874 (Miami-Dade)	73,090 (Monroe)	892	Verizon (84%)	Master Contract – State (41%)	2 (36%)	81%	31%	$50 or Less (80%)	Unlimited (75%)	CAD Interface (84%)
Total	**666**	**38%**	**53 of 67**	**2,662,874 (Miami-Dade)**	**8,365 (Liberty)**	**430**	**Verizon (86%)**	**Master Contract – State (35%)**	**2 (41%)**	**56%**	**26%**	**$50 or Less (80%)**	**Unlimited (83%)**	**One-way Messaging (73%) Internet Browsing (69%)**

This document was prepared by FloridaNet using funds under award 12-10-S13012 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC, or FirstNet.

Contract Vehicle Survey

Thank you for participating in the data collection efforts to design the nations first public safety broadband network. The information collected will be provided to the FloridaNet team for use in the consulation process with FirstNet.

***1. Select your organization type:**

- ◯ Federal
- ◯ State
- ◯ Local
- ◯ County
- ◯ Tribal
- ◯ Private Corporation
- ◯ Public Utilities
- ◯ Public Health Care
- ◯ Other (please specify)

***2. Please select the discipline that best describes your agency or division:**

- ◯ Courts, Corrections and Security
- ◯ Emergency Management
- ◯ Emergency Medical Services
- ◯ Facilities and Land Management
- ◯ Fire Service
- ◯ Highway and DOT
- ◯ Hospitals and Medical Facilities
- ◯ Law Enforcement (Municipal, State, Sheriff, Highway Patrol)
- ◯ Military
- ◯ National Security/Intelligence
- ◯ Public Administration and Support Services
- ◯ Public Health
- ◯ Public Safety Communications
- ◯ Public Utilities (Electricity, Gas, Water, Telecom and Sewer)
- ◯ Specialized Law Enforcement (Investigations, Intelligence, Dignitary Protection, Specific Jurisdiction or Mission)
- ◯ Transportation Services
- ◯ Other (please specify)

***3. Please provide some details about yourself and your organization:**

Name:	
Agency/Organization:	
Address:	
Address 2:	
City/Town:	
State:	
ZIP:	
Position/Title:	
Email Address:	
Phone Number:	

***4. How many of the following types of employees are in your agency? (For the purposes of tracking agency staff, contractors should be considered employees):**

	0-50	51-200	201-500	501-1000	Greater than 1000
Full Time	◯	◯	◯	◯	◯
Part Time	◯	◯	◯	◯	◯
Volunteers	◯	◯	◯	◯	◯

***5. Please provide information on your vehicles used in your agency/organization:**

	0	1-50	51-200	201-500	501-1000	Greater than 1000
Fleet Vehicles that utilize data	◯	◯	◯	◯	◯	◯
Fleet Vehicles that don't utilize data	◯	◯	◯	◯	◯	◯
Personal Vehicles that utilize data	◯	◯	◯	◯	◯	◯
Personal Vehicles that don't utilize data	◯	◯	◯	◯	◯	◯

6. Does your agency/organization utilize any type of data monitoring/data management product?

◯ Yes

◯ No

◯ Not Known

FloridaNet is collecting this data to determine what contract vehicle you utilized to obtain your current wireless broadband data service. Carrier = mobile data carrier

***7. What procurement process was utilized by your agency to select your carrier (select all that apply)?**

- [ ] Master contract - GSA/Federal
- [ ] Master contract - State
- [ ] Master contract - Other entity
- [ ] Local RFP/Bid
- [ ] Based on price quotes
- [ ] Not governed by a formal procurement process
- [ ] Carrier selected by other agency/organization
- [ ] Unknown
- [ ] Other (please specify)

8. How many mobile data carriers are required to fulfill your public safety mission?

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4 or more
- ◯ Not known

9. Why do you require multiple carriers? (check all that apply)

- [ ] Coverage
- [ ] Capacity
- [ ] Features
- [ ] Roaming
- [ ] Redundancy
- [ ] Reliability

Other (please specify)

***10. Please check each of the commercial carriers you use (check all that apply):**

- [ ] AT&T
- [ ] Metro PCS
- [ ] Sprint
- [ ] T-Mobile
- [ ] TracFone
- [ ] US Cellular
- [ ] Verizon
- [ ] Other (please specify)

11. Do you utilize a private data network?

- ◯ Yes
- ◯ No

12. You indicated that you utilize a private data network. Do you own or lease the network?

- [ ] Owned
- [ ] Leased
- [ ] Vendor (please specify)

13. What types of mobile device appliances do you utilize and what is your monthly bill for each?

	Less than $40	$41 - $50	$51 - $65	Greater than $65	N/A
Air card or computer/tablet with integrated wireless modem	◯	◯	◯	◯	◯
Smart Phone	◯	◯	◯	◯	◯
Cell phone (voice only, no data)	◯	◯	◯	◯	◯
USB/Sidecar Modem	◯	◯	◯	◯	◯
Automatic Vehicle Location/ Global Positioning System (AVL/GPS)	◯	◯	◯	◯	◯
Vehicular Modem	◯	◯	◯	◯	◯
Integrated Router	◯	◯	◯	◯	◯

Other (please specify)

14. What type of data plan do you have for these devices?

	Unlimited data	Bundled	Not known
Air card or computer/tablet with integrated wireless modem	◯	◯	◯
Smart Phone	◯	◯	◯
Cell phone (voice only, no data)	◯	◯	◯
USB/Sidecar Modem	◯	◯	◯
Automatic Vehicle Location/ Global Positioning System (AVL/GPS)	◯	◯	◯
Vehicular Modem	◯	◯	◯
Integrated Router	◯	◯	◯

Other (please specify)

*15. Approximately how many devices does each employee have in your organization (devices include laptops with air-cards, tablets, and smart phones)? Please include any personal devices used for work purposes.

- ◯ Less than 1 (a small amount of employees share devices)
- ◯ 1
- ◯ 2
- ◯ 3 or more
- ◯ Unknown

16. What are the most important factors you consider when selecting a mobile data carrier?

	Not at all important	Slightly important	Moderately important	Very important	Extremely important
Cost	◯	◯	◯	◯	◯
Coverage	◯	◯	◯	◯	◯
Capacity	◯	◯	◯	◯	◯
Customer Service	◯	◯	◯	◯	◯
Manageability	◯	◯	◯	◯	◯
Security	◯	◯	◯	◯	◯
User provisioning	◯	◯	◯	◯	◯
Emergency Response	◯	◯	◯	◯	◯

17. What mission critical activities rely on your mobile data network? (check all that apply)

- [ ] Text messaging, paging, one way notifications
- [ ] Automatic Vehicle Location/ Global Positioning System (AVL/GPS)
- [ ] Database inquiries (FCIC/NCIC, criminal history, hot files)
- [ ] Records Management Systems (local queries)
- [ ] Computer Aided Dispatch (CAD) interface
- [ ] Field based reporting
- [ ] Small File transfers (up to 1MB)
- [ ] Large File transfers (over 1MB)
- [ ] GIS/Situational awareness
- [ ] Internet browser access
- [ ] Intranet access/VPN to home network
- [ ] Tactical "chat" rooms
- [ ] Transmission of low quality video
- [ ] Transmission of high quality video
- [ ] Telemetry (continuous process status monitoring)
- [ ] Web based training
- [ ] Video conferencing
- [ ] Mobile device management/updating
- [ ] Land Mobile Radio (LMR) integration

Other (please specify)

Thank you for participating in the FloridaNet contract vehicle survey.

18. What is the level of awareness within your agency of the FloridaNet program?

- ◯ Not familiar at all with the mission, goals and operations
- ◯ Some awareness of the mission, goals and operations
- ◯ Above average knowledge of the mission, goals and operations
- ◯ Extensive knowledge of the mission, goals and operations

This document was prepared by FloridaNet using funds under award 12-10-S13012 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC, or FirstNet

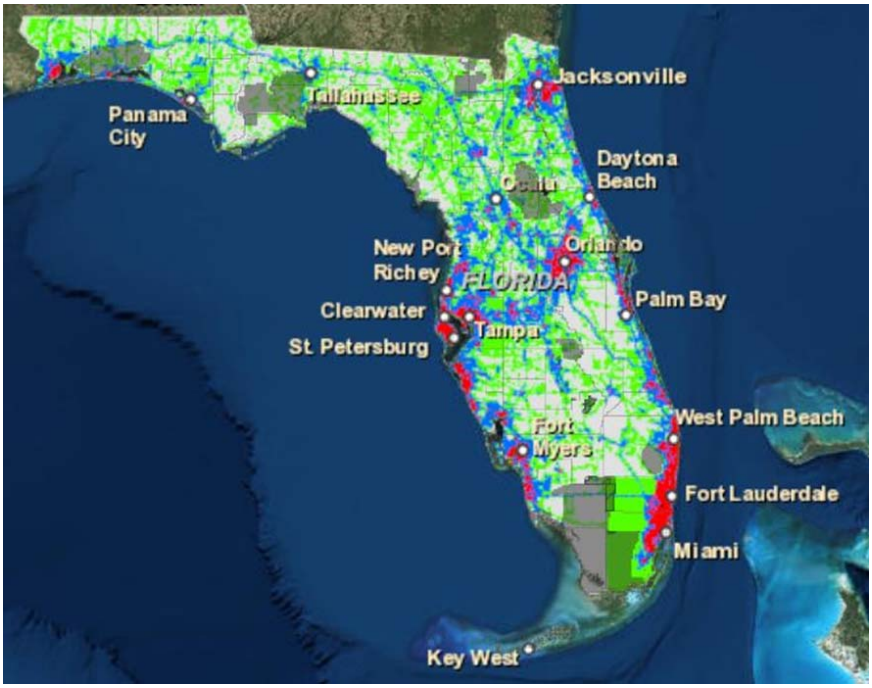
Data Collection

To help identify coverage gaps, or insufficient speeds, found on *FirstNet's Baseline Coverage Objective Map*, a survey was implemented to determine those agencies who had data monitoring tools. Those that did were contacted and asked to provide data that could be sent FirstNet to help inform them on Florida's needs. Once Phase II of the SLIGP grant is awarded, a Request for Quote (RFQ) will be produced to find a vendor to do an extensive data collection throughout the State. This will enable FirstNet to produce a well-informed State plan.

Data that was collected and sent to FirstNet or that will be sent:

- Response areas
- Data usage
- Crash data
- Applications
- Providers
- Computer Aided Dispatch (CAD)

Ninety (90) files, totaling 616 MB, were sent to FirstNet by their deadline of 9/30/15. We are continuing to send files as we receive them. As of 11/4/15, we have sent twenty-eight (28) extra files, totaling 54 MB more. In order ensure that the data we collect survives the end of the grant, we are still moving forward to supply data to CASM NextGen.



FirstNet's Baseline Coverage Objective Map

This is Florida's Baseline Coverage Objective Map, as provided in FirstNet's Draft RFP. The red indicates high concentrations, blue indicates moderate, and the green represents low. The areas not colored in were determined to be out of the scope of terrestrial based coverage. To provide Network access in the non-colored areas, a deployable solution is to be implemented.

FirstNet Data Review

FirstNet reviewed the data that Florida submitted on September 30th. The following are their questions and concerns. Florida responses are in blue.

Sensitive Information

FirstNet: *We are considering making all (or a subset of) data submitted by states available in the Bidders' Library Reading Room as part of our RFP release at the end of the year. This would allow bidders to have direct access to the originally submitted data to further inform their proposals. In doing so, that information would be treated as publicly available information. With that understanding, is there anything in your submission that you would like to have excluded from being shared in a public forum?*

Florida: *Florida has to work under the Sunshine Law, 119, so anything we have submitted is public record and can be shared in a public forum.*

Coverage Objectives and Phasing

Florida provided some of the most detailed response information including aircard usage, consumption, crash, and dispatch data (Data files under the Florida Agencies folder). Can Florida clarify the modifications requested to the baseline Firstnet objective based on this data? No Phased Deployment plan was provided at this time.

User Surveys

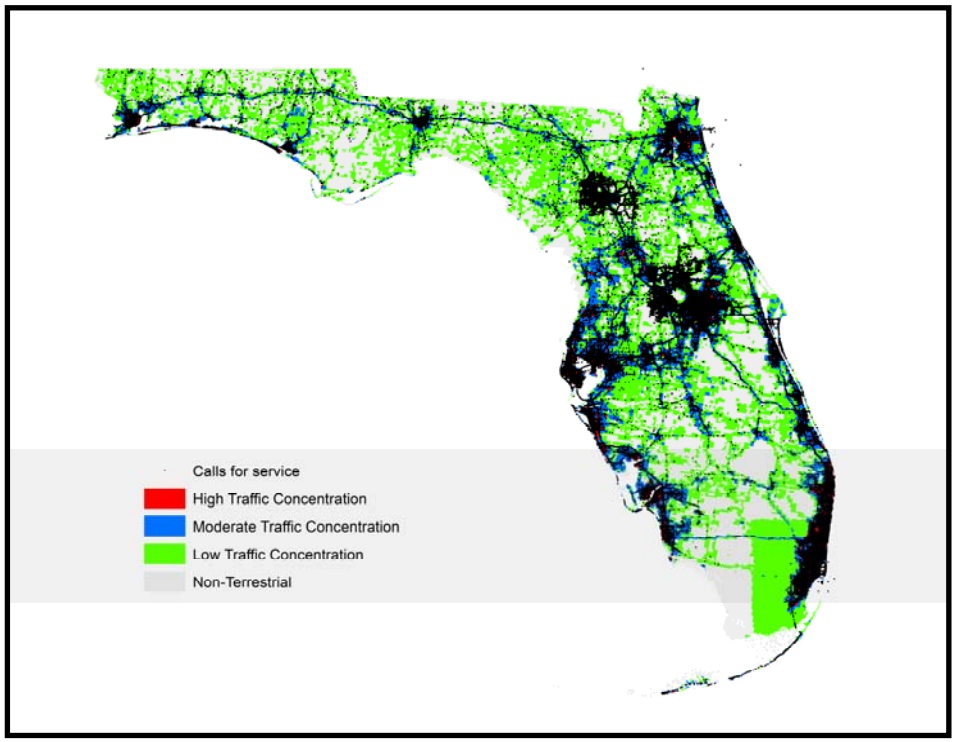
Florida provided detailed survey data on almost 400 agencies (one of the largest survey submissions in the Nation) representing various disciplines and levels of government. The survey information provided personnel/vehicles, applications, procurement and barrier information. The use of ranges for agency personnel and device/user counts (provided as a combined agency and personal use number) will present a challenge in aggregating the data – we would welcome input from Florida on how to most accurately use the State's data in this process.

Total User Estimates

No total user estimates have been provided at this time.

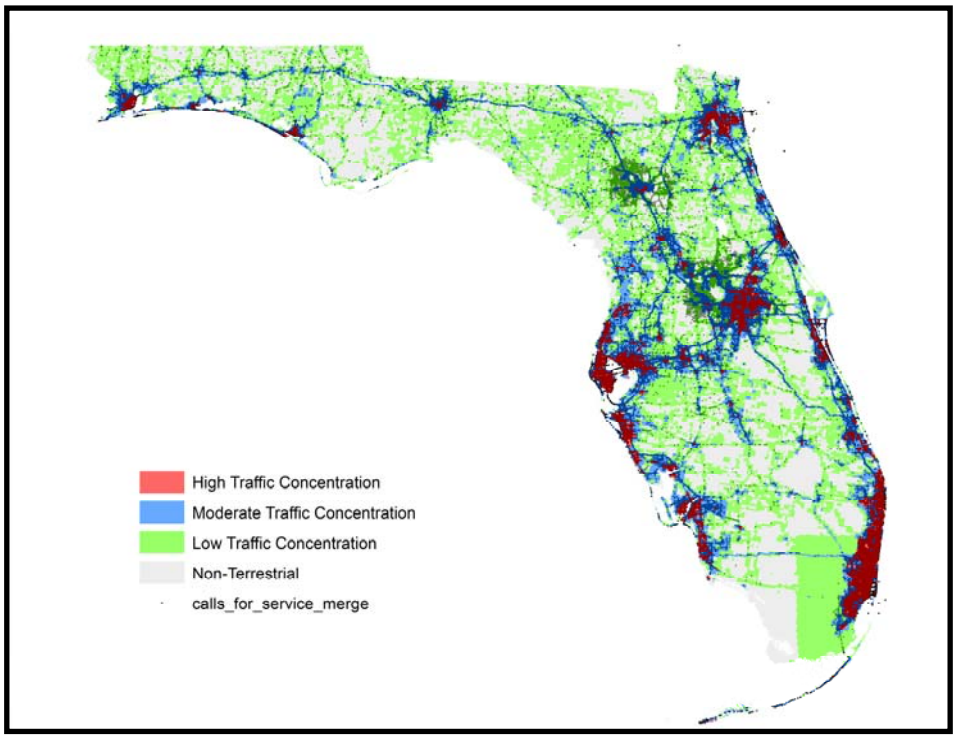
FirstNet Maps

From the data that was submitted, FirstNet was able to input 930,875 Response locations into their maps. The following implements the locations added to the FirstNet Baseline Coverage Objective Map. The maps highlight how the response data can clearly show gaps in the coverage objectives and how the data can be used to fill in those gaps.



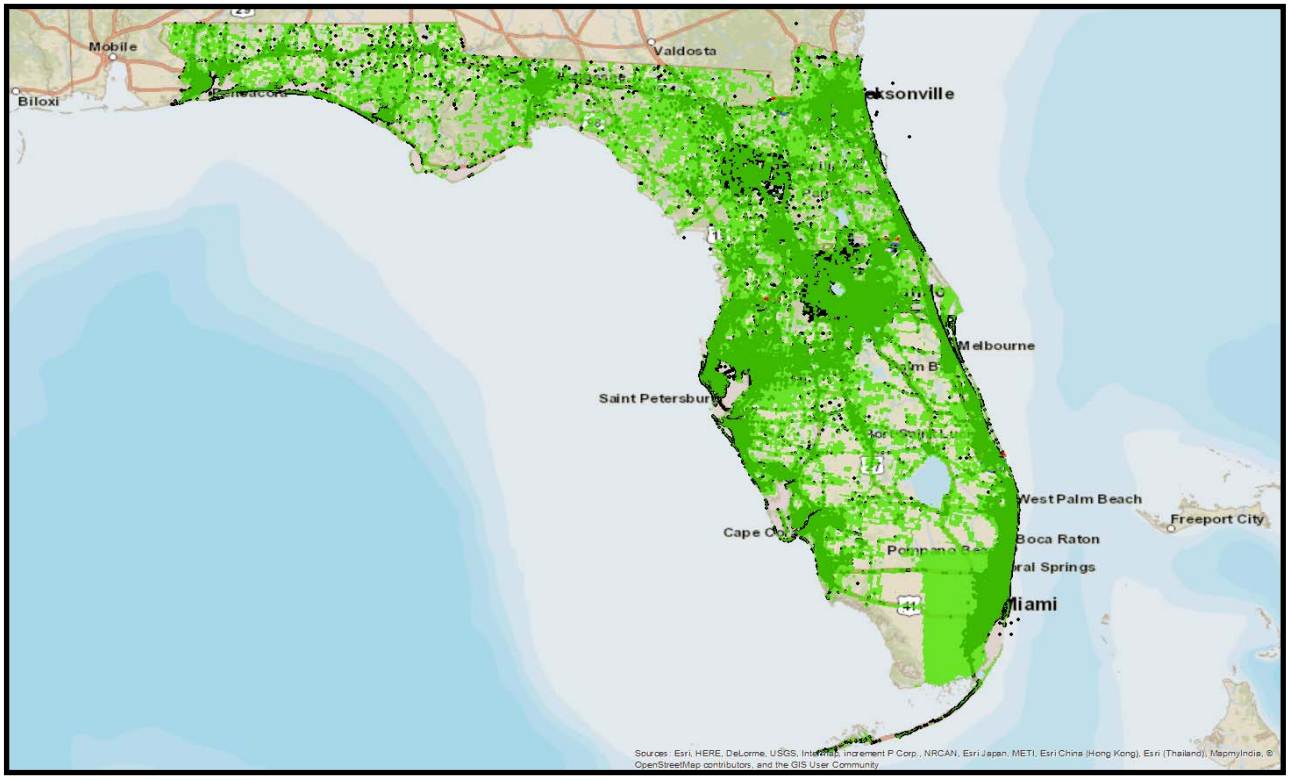
This map shows all the response data on top of the objectives. It shows how the response frequency or concentration correlates to the baseline map. However, FirstNet is not looking to maintain the high/med/low concentration in the final RFP release.

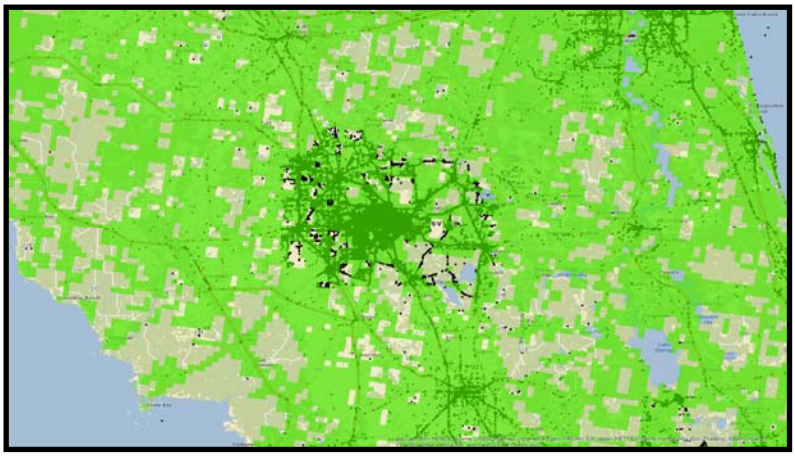
This map shows the objectives on top of the responses data but set to a 50% transparency so you can still see that data underneath. Again, it shows how the data correlates and starts to show gaps in the baseline.



FirstNet Maps

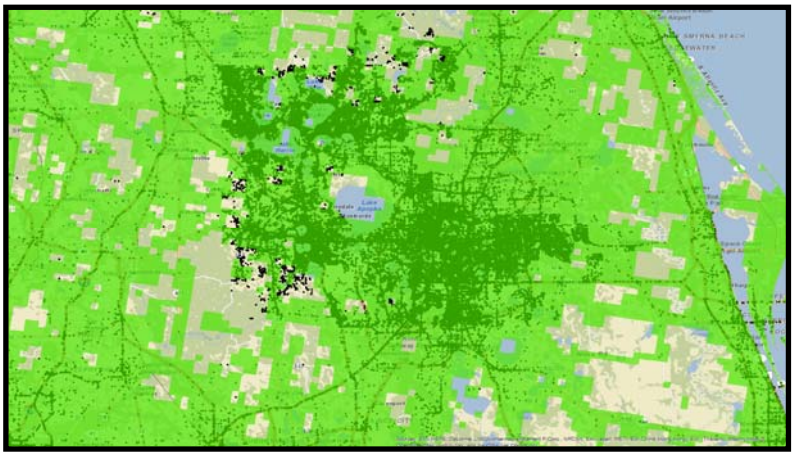
Statewide





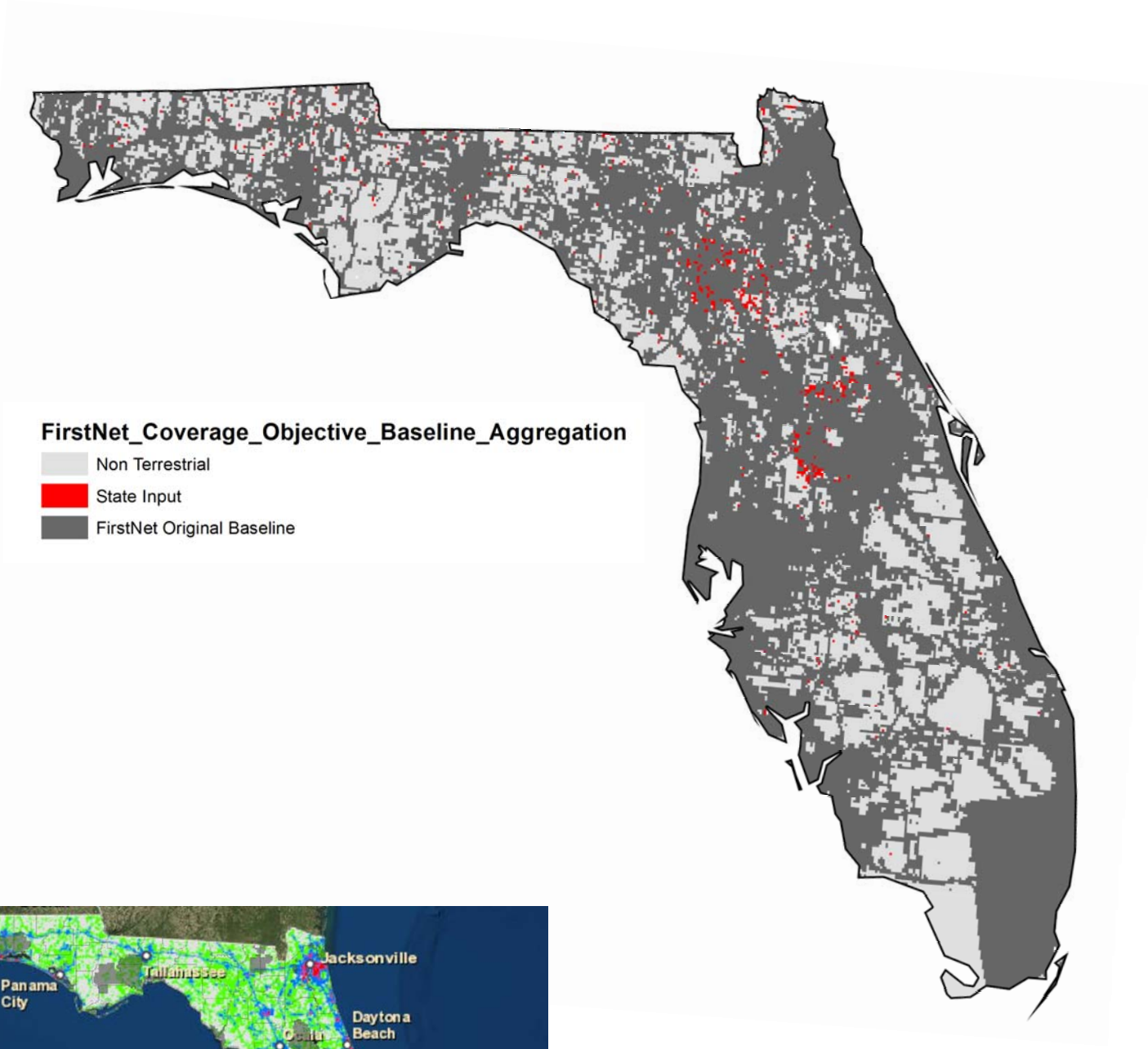
Gainesville Area

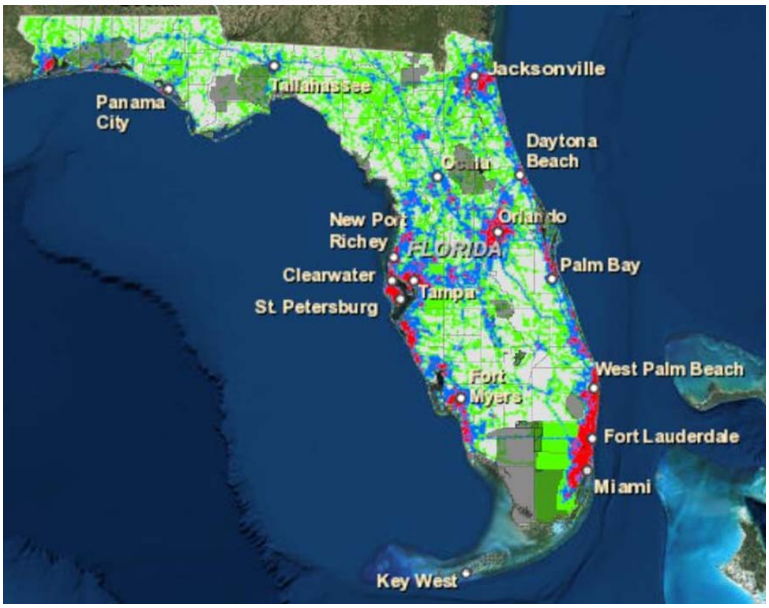
Orlando Area



FirstNet Maps

Updated Baseline Coverage Objective Map





Original Baseline Coverage Objective Map

Budget

Updates

- In March, NTIA announced the availability of Phase II funding
- Instructed the states to prepare a revised budget, budget justification, Baseline/Expenditure Plan, and narrative outlining data collection activities
- Florida's Phase II package was submitted to NTIA prior to August 23rd due date
- Budget is currently being reviewed by NTIA

Significant Changes

- Staffing
    - One full time project planning coordinator to the team as part of the new budget
    - Four part-time regional outreach coordinators
- Data collection contract
    - $1.9 Million for a vendor to assist with on-going data collection, analysis, aggregation and preparation for consultation with FirstNet
    - Vendor solution will also include preparing all Local, State, and Tribal organizations for the consultation process with FirstNet
- Legal Services for potential MOU development
    - $250,000 for legal services to assist in the development of MOUs with Local, State and Tribal organizations on use of existing equipment
    - Goal is to speed build out of network and improve cost effectiveness of the network

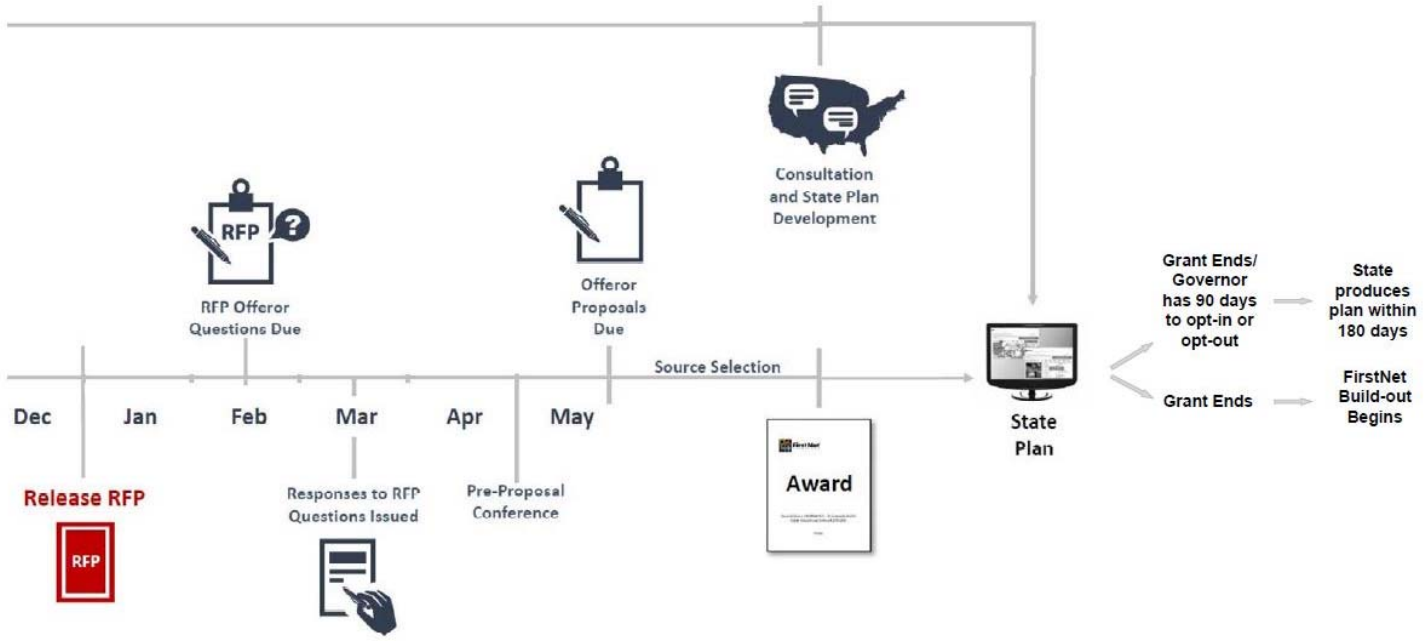
Budget (cont'd)

Breakdown

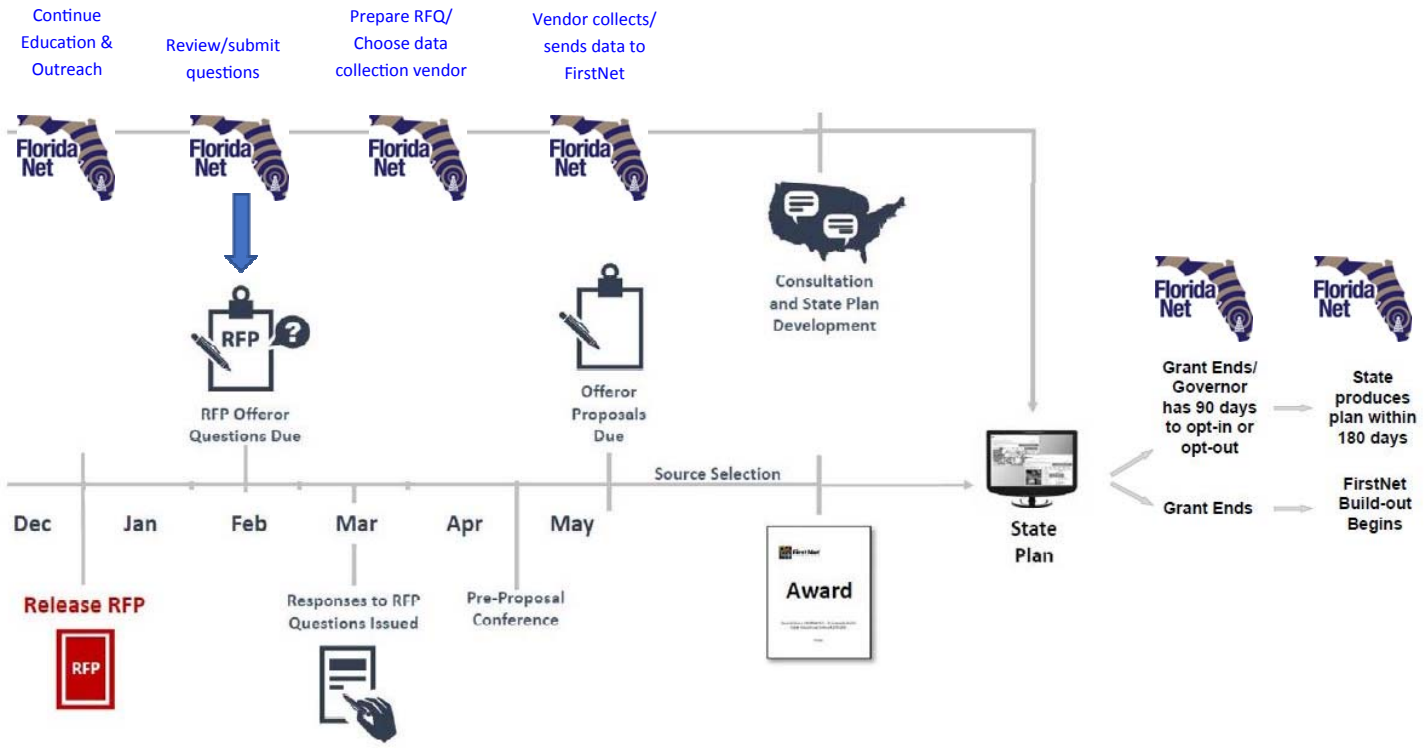
CATEGORY	FEDERAL	STATE MATCH	TOTAL GRANT FUNDS
A. PERSONNEL DEM position	$52,779		$52,779
B. FRINGE BENEFITS DEM fringe benefits	$31,293		$31,293
C. TRAVEL Travel for DEM staff	$9,500		$9,500
D. EQUIPMENT	$0		$0
E. SUPPLIES DEM general supplies	$23,930		$23,930
F. CONTRACTUAL Agreement with DHSMV 8 federally funded positions with benefits 2 positions used as partial match travel for executive committee members and technical committee laptops/software general supplies, printing Phase 2 Data Collection vendor MOU Development Meeting attendance time (match)	$4,768,658	$1,229,010	$5,997,668
G. OTHER DEM collocated costs	$19,110		$19,110
H. TOTAL DIRECT COSTS	$4,905,270		$6,134,280
I. INDIRECT COSTS	$10,770		$10,770
J. TOTAL	**$4,916,040**	**$1,229,010**	**$6,145,050**

Project Plans

FirstNet



FloridaNet



Upcoming Events

Dates

- 12/31/2015 FirstNet to release Final RFP
- 01/09-12/2015 Florida Police Chiefs Association Conference (Ponte Vedra Beach, FL)
- 01/11-15/2015 Southeast Public Safety Broadband Summit (Alabama)
- 04/08/2016 Executive/Technical Committee Meetings *(tentative)*

Next Steps

- Continue to collect data
- Prepare RFQ for Data Collection
- Continue Education & Outreach
- Prepare for Consultation with FirstNet on State Plan

If there are any events in your area that you would like us to attend or present, please let us know!

FloridaNet Executive Committee Meeting

08/28/15

The FloridaNet Executive Committee had a meeting on August 28, 2015 online. The following members and guests participated:

Name	Affiliation
EXECUTIVE COMMITTEE	
Sherri Martin	FL Department of Economic Opportunity
Dr. Peter Pappas, Ex Officio	Health-First, Holmes Regional Medical Center
OTHERS	
Larry Gowen, FloridaNet Director	FL Department of Highway Safety & Motor Vehicles
Alex Perry	FL Department of Highway Safety & Motor Vehicles
Patti Spain	FL Department of Highway Safety & Motor Vehicles
Rhonda MacKinnon	FL Department of Highway Safety & Motor Vehicles
Amy Serles	FL Department of Highway Safety & Motor Vehicles
Kevin Patten	FL Agency for State Technology

Call began at 1:00pm.

Due to Tropical Storm Erika, a majority of members were preparing for emergency response, so the meeting was canceled.