The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress

Jill C. Gallagher
Analyst in Telecommunications Policy

April 27, 2018

Congressional Research Service
7-5700
www.crs.gov
R45179

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

During the events of September 11, 2001 (9/11), first responders could not communicate with each other. Some radios did not work in the high-rise World Trade Center; radio channels were overloaded by the large number of responders trying to communicate; and public safety radio systems operated on various frequencies and were not interoperable. There were also non-technical issues. Officials struggled to coordinate the multi-agency response, and to maintain command and control of the numerous agencies and responders.

The 9/11 Commission called for the "expedited and increased assignment of radio spectrum for public safety purposes." Increased spectrum would allow public safety agencies to accommodate an increasing number of users; support interoperability solutions (e.g., shared channels); and leverage new technologies (e.g., live video streams) to enhance response.

In 2012, Congress acted on the recommendation of the 9/11 Commission. In Title VI of the Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96), Congress authorized the Federal Communications Commission (FCC) to allocate additional spectrum for public safety use; established the First Responder Network Authority (FirstNet) and authorized it to enter into a public-private partnership to build a nationwide public safety broadband network; and, provided $7 billion out of revenues from spectrum auctions to build the network.

February 22, 2017, marked five years since the act was signed into law. FirstNet has made progress in implementing the provisions in the act. In March 2017, FirstNet awarded a 25-year, $6.5 billion contract to AT&T to build and maintain the nationwide network for public safety. FirstNet provided AT&T with 20 megahertz (MHz) of broadband spectrum, which AT&T can monetize for public safety and non-public safety use. AT&T is providing FirstNet access to its infrastructure, valued at $180 billion, and $40 billion to maintain and improve the network.

In September 2017, FirstNet/AT&T presented states with plans detailing how the network would be deployed in each state. Governors could opt to have AT&T deploy the network (i.e., opt in), or have the state assume responsibility for the deployment (i.e., opt out). By January 2018, all 50 states and 6 territories opted in. This was viewed as a victory for FirstNet, AT&T, and public safety stakeholders who had long advocated for a nationwide network for public safety.

However, challenges remain. While governors allowed FirstNet/AT&T to deploy the network in their states, there is no requirement for state and local public safety agencies to use the network. FirstNet/AT&T must attract users to the network to ensure the network is self-sustaining, as required under the act. FirstNet set adoption targets and steep penalties that AT&T must pay if targets are not met. AT&T has offered specialized features and services (e.g., priority access to the network, support during disasters) to attract users to the network. However, Verizon has offered similar services to entice users to its network which may affect FirstNet/AT&T's enrollment efforts. There are other factors affecting enrollment. Some public safety agencies have expressed reluctance to join the FirstNet network, citing uncertainties with the resiliency, reliability, and security of the network, coverage, and cost. Other agencies have expressed an unwillingness to join until FirstNet can provide mission critical voice features—essential features that responders have on their radios and use during emergencies—that will not be available from FirstNet until 2019. Attracting users to the network will be challenging for FirstNet/AT&T, but necessary to meet the requirements in the law and achieve the intent of the act.

Congress may continue its oversight of FirstNet to ensure the FirstNet network is meeting public safety needs (e.g., security, reliability, and resiliency), requirements in the law are met, and the network is deployed as intended. Congress may monitor subscribership to ensure the network will be self-sustaining, as required in the act, and that the intent of the law is achieved.

Contents

Figures

Appendixes

Contacts

Introduction

The First Responder Network Authority (FirstNet) is a federal agency created by Congress in the Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96)—to oversee the building, deployment, and operation of a new nationwide public safety broadband network. In P.L. 112-96 (the act), Congress created FirstNet as an independent authority, within the National Telecommunications and Information Administrations (NTIA), under the Department of Commerce. FirstNet is governed by a Board comprised of federal, private sector, and public safety representatives, which reviews and approves the major decisions of the agency.[1]

Congress authorized $7 billion be allocated out of revenues from spectrum auctions that were authorized in the act. Many in Congress recognized that $7 billion would not be enough to deploy a nationwide network for public safety.[2] As a result, Congress authorized FirstNet to enter into a public-private partnership to leverage commercial infrastructure and services, in exchange for access to FirstNet assets, including $7 billion in funding and 20 megahertz (MHz) of spectrum.

The act is complex. It requires the establishment of a new federal agency and the appointment of a Board of Directors. It requires the development and deployment of a new nationwide broadband network for public safety users. The act requires the auction of spectrum to fund FirstNet—a complex and lengthy process that concluded in 2015. The act requires FirstNet to build the network to industry standards, and the development of technical requirements, some of which were still under development by the international standards development organization, 3GPP.[3] Further, the act requires consultation with public safety users; governors; and federal, state, local, tribal, and territorial entities to coordinate the deployment of the network. Each mandated task took time but was used to inform a request for proposal (RFP) which was released in January 2016, and awarded in March 2017.

In March 2017, FirstNet awarded the contract to build the network to AT&T. In May 2017, AT&T offered public safety agencies priority and preemption services on its nationwide network to attract users to the network.[4] In September, FirstNet/AT&T released state plans detailing the initial (five-year) deployment of the network in the state. By January 2018, all states and territories had opted in to the network (i.e., allowed AT&T to deploy the network in their state).[5]

AT&T is deploying the core network, and plans to deploy the radio access network (e.g., cell site equipment, antennas) in each state. AT&T is also recruiting users to the network to ensure adoption targets are met. FirstNet plans to oversee the network deployment, ensuring: network elements are completed on time, integrated, and interoperable; public safety needs, including coverage, resiliency, and security are met; development and testing of mission critical voice capabilities and devices remain on schedule; user fees and devices are affordable; and that users subscribe to the network, so the network will be self-sustaining.

[1] The Board is comprised of the DHS Secretary, U.S. Attorney General, Office of Management and Budget (OMB) Director, and 12 representatives with various expertise appointed by the Secretary of Commerce (P.L. 112-96 § 6204).

[2] National Public Safety Telecommunications Council, "Senators Worried About Cost of Public Safety Broadband Network," February 16, 2011, http://www.npstc.org/documents/SenatorsWorriedAboutCostPSBBNet110216.pdf.

[3] 3GPP is a (private) standards development organization (SDO) that develops specifications that define 3GPP technologies. For information on 3GPP, see Lair, Yannick and Mayer, Georg, "Mission Critical Service in 3GPP," *3GPP*, June 20, 2017. See http://www.3gpp.org/news-events/3gpp-news/1875-mc_services.

[4] Priority access is a specialized offering that moves first responders to the front of the communications line during periods when communication networks may be difficult to access or congested. Preemption shifts non-emergency traffic to another line to free up space for public safety officials to communicate with others.

[5] For some activities, FirstNet and AT&T acted jointly, which will be depicted in this report as "FirstNet/AT&T."

Background on FirstNet Spectrum

Since the 1920s, first responders have used land mobile radios (LMR), such as radios in vehicles and handheld devices, to communicate during day-to-day operations and emergencies. Radios allow responders to transmit messages quickly over the airwaves to coordinate and communicate during response. To transmit messages over the airwaves, public safety agencies must obtain a license from the FCC which regulates the use of the radio spectrum in the United States.[6]

The FCC assigns frequencies to non-federal users, including state and local public safety agencies. Pursuant to the Communications Act of 1934 (47 U.S.C. § 151 et. seq.), the FCC designated certain segments of spectrum for specific uses. The FCC set aside a swathe of spectrum for public safety; however, demand soon exceeded the amount of spectrum allocated. As a result, the FCC began assigning various frequencies across the radio spectrum to public safety agencies. While the increased assignment of spectrum gave public safety agencies the spectrum they needed to communicate, public safety agencies were now operating on various frequency bands, scattered across the spectrum, using band-specific equipment that was not interoperable with equipment made to operate in other bands. Public safety advocates called for the allocation of additional spectrum and solutions that would enable agencies to interoperate.[7] In the Balanced Budget Act of 1997 (P.L. 105-33), Congress allocated 24 MHz to public safety. This required the transition of broadcasters off the spectrum, but provided an indefinite timeline for their transition; as a result, the spectrum was not immediately available to public safety.

During the terrorist attacks of 9/11, public safety agencies could not communicate with each other. Radio channels were overloaded, and the multiple public safety agencies that responded to the events were operating on various frequencies and could not interoperate. In reviewing the events, the 9/11 Commission confirmed that New York City police and firefighters, operating on different frequencies, and using different channels, could not communicate, which hindered response. Further, the 9/11 Commission noted that systems and channels were overloaded by the large number of responders trying to communicate that day. The Commission called for the expedited and increased assignment of radio spectrum for public safety use.[8]

In the act, Congress provided a large swathe of spectrum, in a single band to enable agencies to communicate and coordinate during emergencies. In the act, Congress reallocated the 700 MHz D Block spectrum from commercial to public safety use.[9] This 10 MHz block was adjacent to an existing block of public safety spectrum that, when combined, provided 20 MHz of prime broadband spectrum to public safety use.

---

[6] In general, spectrum is the range of radio frequencies used for radio, television, and other electromagnetic communications. Specifically, the radio frequency spectrum is the part of the natural spectrum of electromagnetic radiation lying between the frequency limits of 3 kilohertz (kHz) and 300 gigahertz (GHz). Radio frequencies are grouped into bands. Radio signals travel through space in the form of waves. These waves vary in length, and each wavelength is associated with a particular radio frequency. Agencies are assigned specific frequencies by the FCC.

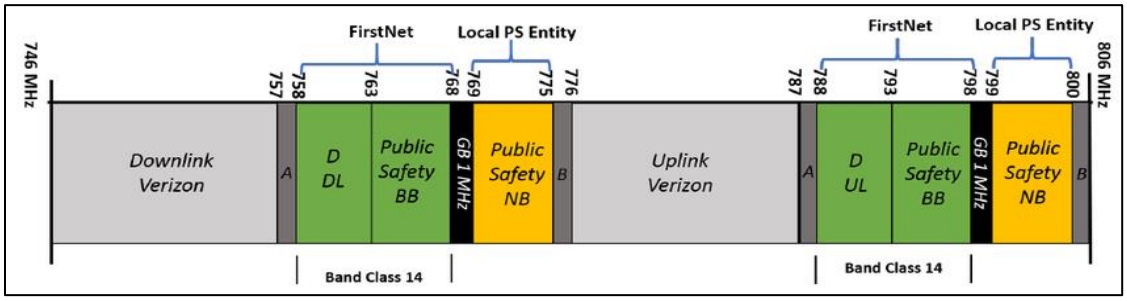
[7] Public Safety Wireless Advisory Committee (PSWAC), Final Report of the Public Safety Wireless Advisory Committee to the Federal Communications Commission and the National Telecommunications and Information Administration, September 11, 1996, https://www.ntia.doc.gov/legacy/osmhome/pubsafe/PSWAC_AL.pdf.

[8] The 9/11 Commission, *The 9/11 Commission Report*, July 22, 2004, p. 397, https://www.9-11commission.gov/report/911Report.pdf.

[9] The 700 MHz spectrum is spectrum available for both commercial and public safety use. The 700 MHz spectrum is considered prime spectrum. Its propagation characteristics allow the 700 MHz signals to penetrate buildings and walls easily and to cover larger geographic areas with less infrastructure. Commercial providers can use this spectrum for mobile broadband services for smartphones, laptops, and tablets.

This combined spectrum (now called FirstNet spectrum or Band Class 14 spectrum) is serving as the foundation for the nationwide public safety broadband network created under the act. **Figure 1** provides an overview of the FirstNet spectrum.

Figure 1. D Block and Public Safety Broadband Spectrum



Source: Kumbhar and Guvenc, *A Comparative Study of LMR and LTE-Based Public Safety Communications,* 2015, Florida International University, Miami Florida, p. 2, researchgate.net.

Notes: Radio spectrum is often grouped in pairs; a block of spectrum in a lower frequency is paired with a block of spectrum in an upper frequency band. One band transmits in one direction (e.g., end-user to the network); this is known as the uplink (UL). Its corresponding pair transmits in the opposite direction (e.g., network to end-user); this is known as the downlink (DL). The green blocks show the paired spectrum that will be used for FirstNet. Also shown is the existing public safety broadband (BB) spectrum (763-768, 793-798 MHz) that was previously allocated for public safety use, and the D Block (758-763, 788-793 MHz) that was allocated to public safety under P.L. 112-96. One pair provides 10 MHz of spectrum (758-768 MHz) to serve as the downlink (DL) for the FirstNet network. The other provides 10 MHz (788-798 MHz) to serve as the uplink. The 10 MHz for the uplink and the 10 MHz for the downlink provide 20 MHz for the FirstNet network. As stipulated in the act, FirstNet holds the license to this paired spectrum (in green). The yellow blocks show narrowband (NB) spectrum assigned to public safety, used for voice communications and nationwide interoperable communications. Guard Bands (GB) of 1 MHz are placed between broadband, narrowband, and commercial carrier spectrum to prevent interference.

This FirstNet (Band Class 14) spectrum is to be used to build out a dedicated public safety broadband network. Broadband is commonly used to mean any high-speed access to the internet.[10] A broadband network for public safety is to provide public safety users with high-speed access to data (e.g., video transfer, internet access) and specialized features and applications (e.g., prioritization of users, location-based services, device management), that are not available on current commercial networks or public safety radios.[11]

While many public safety agencies already use commercial broadband services (e.g., cell phones, laptops), they access these services through commercial providers and commercial networks. During times of heavy use or congestion, which often occurs during emergencies, public safety users face the same constraints as commercial customers—loss of service, network unavailable, inability to make a call due to the high volume of traffic. Public safety users require higher levels of security, reliability, and redundancy to effectively perform their emergency response and life-saving functions. LMR systems have been built to serve public safety users; these are public safety-only systems that provide users with immediate access to the agency's communication system and specialized features for public safety users. Most have, over time, been strengthened

[10] The FCC defines broadband as a connection with speeds of 25 megabits down and 3 megabits up.

[11] Public safety radios provide access to mission critical voice features, such as push-to-talk features, group calling over the radio, direct mode communications which allow responders to communicate off-network with others who are in their vicinity—a useful feature when responders are out of range of their network or when systems are down.

and reinforced to ensure the communication system is reliable, resilient, secure, and protected from natural and man-made disasters. Commercial networks are built to different standards.

Therefore, at any given time, public safety agencies could be using:

- LMR (radio) systems that are owned and operated by individual public safety agencies, serve a specific agency or set of agencies within a certain geographic area, operate on various frequencies across the spectrum, and may or may not be interoperable with other LMR systems in the area. These systems offer reliable *voice* capabilities, are tried and tested in emergencies, have been hardened (i.e., reinforced) to withstand emergencies, and often include back-up capabilities if the network goes down;
- Commercial broadband/cellular networks that are owned and operated by commercial providers, offer nationwide coverage, enable voice communications between users, and offer high-speed access to data and applications, but do not always provide the levels of accessibility, reliability, security, and features that public safety users need; and
- FirstNet is to provide the benefits of commercial broadband networks (e.g., priority access to high-speed data, location-based services, incident management tools), with added reliability, security, and redundancies that public safety needs. At first launch, however, FirstNet will not be able to offer the mission critical voice capabilities that are available through LMR systems; industry standards were approved in May 2016, and device development and testing is underway.[12] Therefore, LMR systems will need to be maintained to ensure public safety has access to mission critical voice capabilities.

State and local public safety agencies leverage different systems to communicate during incidents. FirstNet is intended to supplement these systems, to provide public safety users with dedicated spectrum, added broadband capabilities, and advanced technologies to increase situational awareness and enhance response.

The Value of the FirstNet Spectrum

Congress allocated 20 MHz of valuable broadband spectrum to public safety. As stipulated in the act, FirstNet holds the license to the 20 MHz of spectrum. The act authorizes FirstNet to enter into a public-private partnership and a covered leasing agreement—an agreement to construct, manage, and operate the network. The act also permitted access to network capacity on a secondary basis (i.e., access to the spectrum when it is not in use by public safety).[13]

In its RFP, FirstNet made all 20 MHz of the FirstNet (Band Class 14) spectrum available to the winning bidder. The awardee is permitted to monetize (i.e., earn revenue from) all 20 MHz of the spectrum. As the winning bidder, AT&T can generate revenue from public safety users which must be used to support and improve the network. AT&T can also generate revenue from other users (e.g., secondary users, commercial customers) when the spectrum is not in use by public

[12] *Mission critical voice* capabilities—specialized features that first responders have on their public safety radios and use during emergencies (e.g., push-to-talk features, ability to communicate off-network, emergency calling for first responders)—are not yet available on FirstNet devices. Industry standards for mission critical push-to-talk over LTE (broadband) networks were approved in May 2016 by 3GPP; device development and testing are underway. Therefore, at first launch, mission critical voice features will not be available on the FirstNet network. Public safety agencies will need to maintain their current LMR systems to ensure first responders have access to mission critical voice features.

[13] Sec. 6208 (a) (2)(B)(i) of P.L. 112-96.

safety. Some experts estimated that public safety agencies will use approximately 1% of the FirstNet spectrum, allowing AT&T to use a large portion of the spectrum for commercial use.[14]

In winning the contract, AT&T gained access to 20 MHz of unencumbered nationwide spectrum.[15] Further, the spectrum is not limited to a defined geographical area.[16] Additionally, the spectrum is licensed for *public safety* use, which permits the use of higher powered devices that can provide wider coverage. And, the spectrum does not count against spectrum holding limits set for wireless carriers by the FCC, allowing AT&T to bid on other spectrum.[17] These features add to the value of the FirstNet spectrum, which some experts have estimated to be $8 billion.[18]

AT&T noted that the award of FirstNet aligns with its plan to deploy a commercial 5G network, and that it sees efficiencies that can be achieved from "climbing the tower once" to install equipment for FirstNet, and for its own 5G network;[19] further, the award of FirstNet has provided AT&T with a wider fiber footprint (i.e., a nationwide footprint that includes access to fiber that can connect infrastructure, networks, and devices), which AT&T believes will serve as an advantage during 5G network deployment.[20]

Network Architecture

The act required FirstNet to ensure the establishment of a nationwide, interoperable public safety broadband network (see **Figure 2**), based on a single, nationwide architecture that evolves with technological advancements. Under the act, the network consists of two components:

(1) A core network that

- consists of national and regional data centers, and other elements and functions that may be distributed geographically, and based on commercial standards; and
- provides the connectivity between (i) the radio access network, and (ii) the public Internet or the public switched network, or both.

[14] Trefis Team, "How Much Does AT&T Stand to Gain from FirstNet?," *Forbes*, December 12, 2017, https://http://www.forbes.com/sites/greatspeculations/2017/12/12/how-much-does-att-stand-to-gain-from-firstnet/#78dae0772997.

[15] Unencumbered typically means that the spectrum has been cleared; there are no licensees operating on the spectrum.

[16] The FCC issues licenses to state and local public safety agencies that define not only the frequency on which the agency can operate, but also the geographical area. FirstNet spectrum is not limited to a certain geographic area.

[17] Department of the Interior, *FirstNet Nationwide Public Safety Broadband Network (RFP), Section C: Statement of Objectives*, Solicitation Number: D15PS00295E, Herndon, VA, January 8, 2016, p. C-2.

[18] See Seamus Conwell, "This $15 Billion Spectrum Contract Could Be an 'Issue' for the AT&T Time Warner Deal," CNBC, March 3, 2017, https://www.cnbc.com/2017/ 03/03/this-15-billion-spectrum-contract-could-be-an-issue-for-the-att-time-warner-deal.html. The text says that analysts, including analysts at UBS and Wells Fargo, have estimated the value of the FirstNet spectrum to be $8 billion.

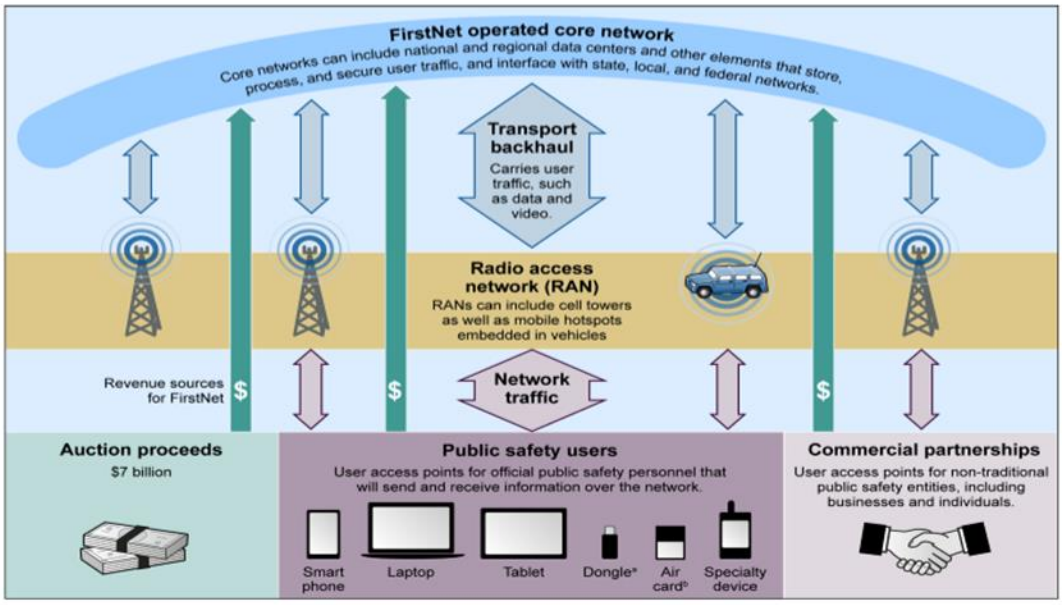
[19] 5G is the next generation wireless technology that promises to provide faster connections, greater bandwidth, extra capacity, quicker download and upload speeds, etc. 5G networks may power self-driving cars, Smart Cities, and connect sensors and other machines. 5G technologies involve the deployment of thousands of small cells (miniature cell towers) on local infrastructure, such as lamp posts, buildings, and other structures.

[20] Securities and Exchange Commission, "Partial Transcript of Q1 2017 AT&T Inc. Earnings Call," April 25, 2017, https://www.sec.gov/Archives/edgar/data/732717/000073271717000049/r425.htm.

(2) A radio access network (RAN) that

- consists of all cell site equipment, antennas, and backhaul equipment, based on commercial standards, that are required to enable wireless communications with devices using the public safety broadband spectrum;
- shall be developed, constructed, managed, maintained, and operated, taking into account the plans developed under the state and local implementation grant program.[21]

Figure 2. Elements of the FirstNet Network



Source: U.S. Government Accountability Office, *Public-Safety Broadband Network: FirstNet Should Strengthen Internal Controls and Evaluate Lessons Learned,* GAO-15-407, April 28, 2015.

Note: Figure 2 depicts the elements of the FirstNet network, and the flow of information between the elements. For example, Public safety users can use a variety of devices to access the FirstNet network. The message flows from the public safety user's device to the radio access network (RAN), which include cell towers, mobile units in cars, and backhaul (e.g., fiber that can transport messages). The messages are carried to the core network which can include regional data centers and other infrastructure that processes, stores, and secures the data, and can enable interconnections with federal, state, and local networks, as well as the internet. Figure 2 also shows revenue that will be used to support the network including auction proceeds ($7 billion), and the private partner contribution, which will be $40 billion over the 25-year span of the contract.

FirstNet, with its private partner (AT&T), is responsible for building the core network. The core is a key component for ensuring that users have a consistent experience nationwide, and that the network is interoperable. Through the core, FirstNet can ensure a centralized approach to managing access, uniform user profiles, applications and services; further, FirstNet can consistently manage information and users and ensure the security of network. The RAN portion of the network (i.e., cell towers, hot spots embedded in vehicles) is to be deployed state-by-state. Traffic is to flow from devices (e.g., smart phones, tablets) through the RAN and is to backhaul to the core network over satellite or other wireless infrastructure.[22]

[21] State and Local Implementation Grant Program: https://www.ntia.doc.gov/sligp/program_information.

[22] Backhaul refers to links that carry user traffic (e.g., voice, data, video), and signaling from base stations to the core.

The act requires the network to comply with minimum technical interoperability requirements, set by an Interoperability Board, and based on commercial standards for Long Term Evolution (LTE) service.[23] The act encourages the use of commercial and government-owned infrastructure to speed the deployment of the network, and permits FirstNet to enter into roaming agreements, which would allow users to make and receive calls when traveling outside the geographic coverage area of the FirstNet network. The act also requires rural coverage milestones be set throughout each phase of deployment, to ensure agencies in rural areas have access to FirstNet.

Major Developments in 2017

On March 30, 2017, FirstNet awarded AT&T with a 25-year contract to build, operate, and maintain the nationwide public safety broadband network.[24] Under the agreement, FirstNet will provide $6.5 billion to AT&T over the first five years, and access to 20 MHz of broadband spectrum (also called FirstNet spectrum or Band 14 spectrum, discussed above). AT&T will provide FirstNet with access to its existing infrastructure, valued at more than $180 billion, and with $40 billion over the life of the contract to support the public safety network.

Under the contract, AT&T will build a 4G Long Term Evolution (LTE) network for public safety users. AT&T has a five-year deployment plan, which includes the development and deployment of the core network, and the deployment of the radio access network (RAN) in each state and territory. During the deployment period, AT&T has offered public safety users access to its commercial network with priority and preemption services. Priority access means that public safety users can access AT&T's commercial network during emergencies, when there is typically heavy use and congestion.

In June 2017, FirstNet/AT&T provided states with preliminary state plans, detailing how FirstNet/AT&T would deploy the Radio Access Network (RAN) portion of the network in each state (e.g., cell towers, mobile hot spots). The deployment plans were based on state and local needs, and other information collected during consultations between FirstNet and states over the past three years. Plans included information on the network architecture, including coverage and pricing—two critical elements driving state decisions to opt in or out of the network.[25] States provided feedback to FirstNet/AT&T, which was used to prepare the final state plan.

On September 29, 2017, FirstNet/AT&T released final plans to the states. As required in the act, FirstNet sent an official notice to each governor, which triggered a 90-day review of the state plan. Governors could accept the FirstNet/AT&T plan for the build-out of the network in their state (i.e., opt in), *or* issue a Request for Proposal (RFP) to build its own RAN (i.e., opt out). After consideration of the costs and benefits, all 50 states and 6 territories opted in.[26]

[23] LTE is a standard for wireless communications set by 3GPP that indicates a streamlined network architecture, roaming on other networks, and faster connections for users accessing applications and multimedia on mobile devices.

[24] The award was delayed for several months, after Rivada Mercury unsuccessfully challenged the selection process in the U.S. Court of Federal Claims. See *Rivada Mercury, LLC v. The United States of America and AT&T Corp.*, 16-1559C (U.S. Court of Federal Claims 2017), https://ecf.cofc.uscourts.gov/cgi-bin/show_public_doc?2016cv1559-87-0.

[25] Testimony of Mr. Curtis Brown, in U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *An Update on FirstNet*, hearings, 115th Cong., 1st sess., July 20, 2017.

[26] It is important to note that while the governor or territorial leader may have opted in to FirstNet (i.e., allowed AT&T to deploy the network in the state or territory), state and local public safety agencies (e.g., state police, local fire departments) are not required to subscribe to the network (i.e., use the network).

Additional developments in 2017 included:

- **Spectrum Relocation.** The National Telecommunications and Information Administration (NTIA) worked with public safety agencies that were operating in the FirstNet spectrum (Band Class 14) to relocate those licensees to other 700 MHz spectrum, to clear the spectrum for the FirstNet network. NTIA awarded nearly $27 million through its Spectrum Relocation Grant Program to fund relocation costs. As of April 2018, 8 of 10 funded projects are complete.
- **Public Safety Broadband Research.** The National Institute of Standards and Technology (NIST) awarded $38.5 million under the Public Safety Innovation Accelerator Program, to 33 entities to conduct public safety broadband research. This program received $300 million funded from revenue generated by spectrum auctions authorized in the act. The $38.5 million represents the first round of public safety broadband research awards.
- **Next Generation (NG911) Grant**. In September 2017, NTIA and the Department of Transportation's National Highway Traffic Safety Administration (NHTSA) proposed rules for the NG911 program funded from revenue generated by spectrum auctions authorized in the act. The grant is aimed at improving state and local 911 technologies and services. NTIA and NHTSA are finalizing the rules and expect to release the grant notice in 2018.
- **State and Local Implementation Grant Program (SLIGP).** In 2017, NTIA announced a second round of funding (SLIGP 2.0). SLIGP 2.0 can fund personnel to help coordinate FirstNet activities, including identifying users, establishing governance structures, conducting data collection, and developing policies to increase data sharing across public safety systems. Every state and territory is eligible for SLIGP 2.0 funding. The grants have a 20% matching requirement, a two-year period of performance, and are to be awarded in 2018.
- **Tribal Consultation.** In October 2017, FirstNet released a *Tribal Consultation Policy*, establishing a nation-to-nation relationship between tribes and FirstNet, to ensure effective consultation with tribes during the build-out of the network. The policy was developed in accordance with Executive Order 13175 which sets core principles for engaging with federally-recognized tribes. [27]

Issues for Congress

In 2017, Congress conducted oversight hearings on FirstNet.[28] Some Members questioned FirstNet, AT&T, and state representatives on state plans, the opt-in/opt-out process, factors affecting opt-in/opt-out decisions, and critical aspects of the FirstNet/AT&T network, including coverage (rural and non-rural); the security, reliability and redundancy of the FirstNet network; features available on the network; site hardening (e.g., strengthening and protecting critical infrastructure from disasters); and cost. These issues were also raised by states during the review

[27] Executive Order 13175, "Consultation and Coordination with Indian Tribal Governments," (Washington: GPO, 2000), https://www.gpo.gov/fdsys/pkg/FR-2000-11-09/pdf/00-29003.pdf.

[28] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, 115th Cong., 1st sess., July 20, 2017; and U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Communications, Technology, Innovation, and the Internet, *Oversight of FirstNet: State Perspectives*, 115th Cong., 1st sess., November 1, 2017.

of their state plans, and may indicate issues affecting public safety agencies' decisions to use the FirstNet network, which is essential to its long-term sustainability.

The act requires that the network be self-sustaining through user fees, but it does not require public safety agencies to subscribe to the network. Congress may provide oversight of FirstNet to ensure that the network is being deployed as required in the act and as intended by Congress. Congress may also monitor the deployment to ensure that FirstNet/AT&T are meeting public safety needs and providing features and services that will attract users to the network. Users are needed to ensure that the network will be self-sustaining, as required in the act, and to achieve the intent of the law—to provide a single, interoperable network that public safety agencies can use to communicate and coordinate during disasters.

In providing oversight, Congress may consider the following issues.

Transparency of AT&T Contract

The FirstNet RFP was released in January 2016. The RFP did not dictate how the network should be deployed; instead, the RFP asked bidders to provide their own innovative solutions to achieving sixteen high-level objectives included in the RFP by FirstNet.[29] AT&T was awarded the contract in March 2017 based on its innovative approach, technical capability, and financial stability; however, the contract was deemed proprietary and was not available for public view. Since there is no specific approach delineated in the RFP, and since the actual approach is not available for public review, it is likely difficult for Congress to understand how the FirstNet network will be deployed. A number of Members of Congress have sought clarity on several aspects of the network. For example, during recent congressional hearings, some Members asked how and where the FirstNet network will be deployed; how FirstNet/AT&T will meet rural coverage requirements in the act; and if the AT&T solution provides the security, reliability, and resiliency that public safety agencies need during emergencies.[30] Without access to the contract, or greater details on the deployment, it is likely difficult for Congress to ensure that the requirements in the act are being fulfilled, and that the intent of the law is met.

Further, the RFP required FirstNet/AT&T to develop state plans which detailed the deployment of the radio access network (RAN) in each state. The state plans provide information on the coverage provided by AT&T, the deployment schedule, the services and devices available to users, and the cost to users. FirstNet/AT&T released preliminary plans in June 2017. Like the contract, the state plans were also deemed proprietary. Plans were made available to select state officials through a secure portal that required users to accept lengthy terms and conditions, including a non-disclosure agreement. Since the state plans were not released, it is not possible to analyze the plans, or to compare coverage, services, and pricing between states. Without insight into state plans, it will likely be difficult for Members of Congress to understand the FirstNet deployment plan for their state, to analyze how funding and other resources have has been distributed across states, or to ensure that requirements in the act are met.

This $6.5 billion, technically and financially complex project was proposed by Congress in response to the communication challenges experienced during 9/11 and other incidents. Given its

[29] For example, FirstNet required that the network serve users nationwide and be interoperable; be deployed quickly; be secure; and that a variety of devices must be offered, etc. The RFP did not provide "one right way" to achieve these objectives but allowed the bidders to present their own solution to achieving these objectives.

[30] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, 115th Cong., 1st sess., July 20, 2017, https://www.commerce.senate.gov/public/index.cfm/hearings?ID=28BA6F3B-F540-4373-8DC8-7C42006FBC81.

size and the importance of the network to the life and safety of first responders and citizens, the current proprietary nature of the detailed plans for the project may hinder the ability of Congress to conduct effective oversight. Congress may consider requiring FirstNet to release the contract and state plans, or to provide greater detail on the network, so that Congress can ensure that the FirstNet/AT&T approach meets the requirements in the act, and the intent of the law: to provide a nationwide network for public safety to communicate and coordinate during response.

Core-to-Core Interoperability

Throughout the development of the FirstNet RFP, public safety advocates and industry experts debated whether there should be one nationwide vendor for FirstNet, or if there could be multiple vendors, and multiple interconnected cores that comprise the FirstNet network.[31] After receiving extensive input from public safety advocates and industry experts, FirstNet/AT&T decided on a comprehensive solution (i.e., one-vendor, nationwide solution), which it included in its RFP. After the award of the RFP, several commercial providers advocated for the interconnection of other cores to the FirstNet/AT&T core.[32] This would allow commercial providers to retain their public safety customer base and allow users access the FirstNet network, when needed.

AT&T argued that the RFP required the "provisioning of a [single] nationwide core," and did not allow for multiple core networks, and integrating multiple cores into the nationwide network would increase cyber risks.[33] FirstNet agreed with AT&T and re-stated the need for a single core, "to reduce the risk of complications inherent in a multi-core architecture (operated by distinct entities), such as operational complexity, security complexity, and increased latency."[34]

While the idea of core-to-core interoperability seemed to be rejected, the issue resurfaced when Verizon announced in August 2017 that it would be building its own dedicated, public safety core network for public safety customers.[35] Like AT&T's core, the Verizon core plans to operate separately from its commercial core, and provide first responders with access to the company's extended LTE network, and priority and preemption services. Verizon intends to also make available multi-band devices that will provide access to any Band Class 14 RAN deployed by FirstNet and committed (as did AT&T) to investing in new broadband technologies for its public safety customers.[36] Verizon appears to be offering a parallel service to FirstNet and continues to advocate for interconnections with the FirstNet/AT&T core.[37]

FirstNet has stated that its one-vendor approach will allow it to achieve efficiencies in management, procurement, deployment, and operation of the network. Some public safety

[31] CRS Report R42543, *The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress*, by Lennard G. Kruger.

[32] See Letter from Mr. Declan Ganley and Mr. Joseph J. Euteneuer, Rivada Networks LLC, to Ms. Marlene Dortch, Secretary, FCC, June 12, 2017, https://ecfsapi.fcc.gov/file/106122435010907/ FCC%20ex%20parte% 20letter%20 FINAL%206-12-17.pdf.; and see Verizon blog, "Verizon to Build Dedicated Network Core for Public Safety," August 16, 2017, http://www.verizon.com/about/news/verizon-build-dedicated-network-core-public-safety.

[33] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Communications, Technology, Innovation, and the Internet, *Oversight of FirstNet: State Perspectives*, 115th Cong., 1st sess., November 1, 2017, https://energycommerce.house.gov/hearings/oversight-firstnet-state-perspectives/.

[34] FirstNet, "Facts About FirstNet: Our Nation's Public Safety Broadband Network," https://www.firstnet.gov/facts.

[35] Letter from Donald Brittingham, Verizon, to Subcommittee on Communications and Technology, October 31, 2017, http://docs.house.gov/meetings/IF/IF16/20171101/106569/ HHRG-115-IF16-20171101-SD007-U7.pdf.

[36] See Verizon advertisement during 2018 Super Bowl, https://www.youtube.com/watch?v=ipx4Wu5P_lE.

[37] Letter from William H. Johnson, Verizon, to Ms. Marlene Dortch, Secretary, FCC, July 24, 2017, https://ecfsapi.fcc.gov/file/10724307201497/2017%2007%2024%20 Verizon%20FirstNet%20FCC%20letter.pdf.

advocates supported this approach;[38] others have argued that competition is good—that it will reduce costs, increase options, and spur innovation for public safety users.[39]

FirstNet and AT&T have expressed concern that the integration of other networks into the FirstNet network may affect security, interoperability, and sustainability of the network.

- **Security:** FirstNet and AT&T have stated that integrating other core networks that may not adopt and enforce the same technical requirements, protocols, training, and best practices could jeopardize security.[40]
- **Interoperability:** Verizon argued that the Technical Advisory Board created under the act to advise FirstNet on interoperability, *allowed* interoperability through "core-to-core interconnection and mutual automatic roaming arrangements…."[41] Further, Verizon stated that secure interoperability is feasible, and that a competitive marketplace spurs innovation.[42] AT&T noted interoperability between cores may be *technically* feasible, but it has not yet been attempted between commercial carriers, and brings security risks; further, AT&T argued that this approach does not serve the requirement in the act to create an interoperable nationwide network based on a single, nationwide architecture.[43] FirstNet agreed with AT&T, noting that there is uncertainty in how core-to-core connections would affect interoperability and security.[44]
- **Sustainability:** In its 2017 Report, GAO noted that if commercial carriers compete, it may affect the state and local adoption of (and subscription to) the network, which could affect the long-term sustainment and improvement of the network. Verizon has already amended its service offerings to include priority service and a preemption offering to public safety users, in order to sustain its customer base. While the interoperability of cores may spur competition and reduce costs, it may also negatively affect subscriptions to FirstNet and the long-term viability of the network.

In the act, Congress required the network to be secure, interoperable, and self-sustaining. FirstNet/AT&T has adopted policies to ensure those requirements are met. However, questions on core-to-core interoperability remain. The development of a separate core by Verizon—which has stated that it services two-thirds of the public safety market—may affect subscribership to the FirstNet network, and threaten its long-term sustainability. Congress could mandate integration of the cores to increase the number of users on the network; however, it may seek to clarify if AT&T is planning on integration other cores, and to gain more information on the financial and security

[38] APCO, "APCO Welcomes Publication of FirstNet's RFP," January 13, 2016, https://psc.apcointl.org/2016/01/13/apco-welcomes-publication-of-firstnets-rfp/.

[39] Testimony of Mr. Robert LeGrande, in U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Communications and Technology, *Oversight of FirstNet: State Perspectives*, hearings, 115th Cong., 1st sess., Nov. 1, 2017, http://docs.house.gov/meetings/IF/IF16/20171101/106569/HHRG-115-IF16-20171101-SD001-U1.pdf.

[40] FirstNet, https://firstnet.gov/content/firstnet-will-provide-public-safety-users-priority-access-network#Security.

[41] Letter from William H. Johnson , Senior Vice President, Federal Regulatory and Legal Affairs, Verizon, to Ms. Marlene Dortch, Secretary, FCC, July 24, 2017, https://ecfsapi.fcc.gov/file/10724307201497/2017%2007%2024%20Verizon%20FirstNet%20FCC%20letter.pdf.

[42] Mike Maiorana, Senior Vice President, Verizon Enterprise Solutions, "Interoperability Will Work for Public Safety," *LinkedIn*, September 28, 2017, https://www.linkedin.com/pulse/interoperability-work-public-safety-michael-maiorana/.

[43] Donny Jackson, "AT&T Exec Discusses Core-to-Core Interoperability, Verizon Proposal, FirstNet Differentiators," *Urgent Communications*, August 17, 2017, http://urgentcomm.com/public-safety-broadbandfirstnet/att-exec-discusses-core-core-interoperability-verizon-proposal-first.

[44] Donny Jackson, "Verizon Meets with FirstNet, but Interoperability Questions Remain," *Urgent Communications*, October 3, 2017, http://urgentcomm.com/ntiafirstnet/verizon-meets-firstnet-interoperability-questions-remain.

impact of integrating other cores into the FirstNet core.[45] Congress may also encourage and support subscribership to the FirstNet network through other means; for example, Congress could provide grant funding to state and local public safety agencies to purchase FirstNet devices.

Services Beyond the Initial Five-Year Deployment

By January 2018, all 50 states and 6 territories accepted the FirstNet/AT&T plan to deploy the network in their state, although some opted in reluctantly.[46] Many states opted in and noted that there were outstanding items that were not fully addressed in state plans (e.g., future coverage, site hardening, improvements), that needed to be discussed with FirstNet and AT&T and addressed either in the five-year initial deployment or in the out-years. FirstNet and AT&T stated that they could not address all state and local public safety needs during the initial five-year deployment, but that they would continue to work with states to address outstanding issues.

Congress may continue its oversight of the FirstNet network through the initial five-year deployment of the network, and after. FirstNet has a contract with AT&T for 25 years. The act requires that revenues earned from public safety users be invested back into the network for improvements. Congress may clarify with FirstNet and AT&T how and where revenues will be used to improve the network. Congress may consider inviting state and local public safety agencies to testify at oversight hearings to hear whether issues not fully addressed in state plans or addressed in the initial five-year deployment (e.g., coverage, rural coverage, rural partnering agreements, site hardening, resiliency, security), are being adequately addressed in the out-years.

Coverage

Coverage has been a key issue for public safety since the network's inception. Without coverage, public safety agencies will not be able to use the FirstNet network to coordinate and communicate with others during emergencies. And, without coverage, agencies will not subscribe to the FirstNet network, hindering FirstNet's ability to ensure the network is self-sustaining as required under the law. In the act, there are no quantitative coverage requirements; however, the act does require substantial rural coverage milestones be set with each phase of deployment, and requires FirstNet to consult with state, tribal, and local entities regarding coverage needs.

In the RFP, FirstNet included two major provisions on coverage—a short term requirement to provide public safety with access to nationwide coverage within six months of award, to speed adoption of broadband, as encouraged under the act. And, a requirement to provide a longer-term, five-year deployment plan, with rural coverage milestones for each phase of deployment, as required under the act. While the provisions in the RFP reflect the requirements in the act, the proprietary nature of the contract and the state deployment plans makes it difficult to determine if the requirements of the law are being met, how the resources provided (e.g., $6.5 billion and 20 MHz spectrum) are being used, and if the network is being deployed as intended by Congress.

For the short-term deployment plan, FirstNet required the contractor to provide nationwide coverage, using the Band Class 14 spectrum (FirstNet spectrum) or other spectrum (non-Band

[45] The act requires partnerships with rural providers which may own and operate their own cores; several pilot projects were funded in 2012 to test LTE technologies in anticipation of FirstNet—some of these projects deployed their own cores which may need to be interconnected to FirstNet's core; additionally, there may be unique telecommunications agreements (e.g., providers that service the Pacific territories) that may require core-to-core interconnections.

[46] Letter from Mark S. Ghirlarducci, Director, CalOES, to Michael Poth, CEO, FirstNet, December 28, 2017, http://www.oesnews.com/wp-content/uploads/2017/12/California_FirstNet_Decision_Letters_2017-12-28.pdf.

Class 14), within six months of award. This provision allows the contractor to provide nationwide coverage by either building out the new nationwide network on Band Class 14 spectrum (FirstNet spectrum) or to provide nationwide coverage using their own spectrum and networks. This provision was intended to speed delivery of broadband to public safety agencies, as encouraged under the act, and to offer a nationwide solution while the FirstNet network was being built, which is expected to take five years for the initial deployment.

After the contract was awarded, AT&T announced that it would open *all* its spectrum bands that are LTE-enabled (i.e., all of its broadband spectrum) for public safety use and provide priority and preemption services to public safety users who subscribed to the FirstNet network. This would provide public safety users with immediate access to broadband services, access to a nationwide network, and assurances that public safety communications would be prioritized on AT&T's commercial network during emergencies.

Some proponents viewed the announcement as an opportunity to access commercial broadband services sooner, before the deployment of the FirstNet network, with the assurances that public safety communications would be prioritized on the AT&T network. Others saw AT&T's offer as a means to increase capacity (e.g., enable more users on the network), and to relieve congestion on crowded radio channels. Some argued that AT&T's approach could provide public safety agencies with flexibility to leverage new technologies (e.g., 5G) that may operate outside the 700 MHz band, as they become available.[47] Critics asserted that AT&T is using its commercial network as a base for the nationwide public safety broadband network—"rebranding" the AT&T network as the FirstNet network,[48] instead of building a dedicated public safety broadband network in Band Class 14, as intended in the act.[49]

AT&T stated that it is building out Band 14 as agreed to in the contract; this statement is supported by the RFP which requires that, six months from award, the contractor shall provide nationwide coverage on Band Class 14 *or* Non-Band Class 14. However, the discussion around this topic raised questions as to when and where AT&T *would* be deploying Band Class 14 (FirstNet) network, and how the 20 MHz of spectrum allocated to public safety is being used.

In a July 2017 hearing of the Senate Subcommittee on Communications, Technology, Innovation, and the Internet, Senators asked where the Band Class 14 infrastructure would be deployed, and percentage of land covered.[50] AT&T stated that Band Class 14 will be deployed in areas where AT&T determines there is a need for additional capacity but declined to provide details on the deployment due to proprietary reasons. In later statements, AT&T later reported that the Band Class 14 network (i.e., the FirstNet network) will be deployed not only where there is a need for greater capacity (i.e., areas of high-density), but also on new sites to cover rural areas that are

[47] Donny Jackson, "Unanswered Questions Loom as Governors Prepare to Make 'Opt-In/Opt-Out' FirstNet Choices," *Urgent Communications*, October 4, 2017, http://urgentcomm.com/blog/unanswered-questions-loom-governors-prepare-make-opt-inopt-out-firstnet-choices.

[48] Albert J. Catalano, "Has FirstNet Rebranded AT&T's Network as the Nationwide Public Safety Broadband Network?," *National Law Review*, August 29, 2017, https://www.natlawreview.com/article/has-firstnet-rebranded-att-s-network-nationwide-public-safety-broadband-network.

[49] Donny Jackson, "Unanswered Questions Loom as Governors Prepare to Make 'Opt-In/Opt-Out' FirstNet Choices," *Urgent Communications*, October 4, 2017, http://urgentcomm.com/blog/unanswered-questions-loom-governors-prepare-make-opt-inopt-out-firstnet-choices.

[50] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, 115th Cong., 1st sess., July 20, 2017, https://www.commerce.senate.gov/public/index.cfm/hearings?ID=28BA6F3B-F540-4373-8DC8-7C42006FBC81.

unserved or underserved.[51] AT&T also stated that deployable assets would be used to provide coverage to areas, when needed.

AT&T stated that they will cover more than 99% of the population, and 76.2% of the geography without deployable assets.[52] By combining the AT&T wireless LTE network with rural networks, deployable assets,[53] and additional satellite technology, FirstNet/AT&T stated that it will be able to cover more than 99% of the U.S. geography.[54]

While deployable solutions can offer coverage immediately following emergencies, they are not counted as persistent coverage toward rural milestones, nor do they serve as permanent communication solutions. Deployable assets take time to deploy and can be moved to serve another jurisdiction or agency if an emergency arises.

Without detailed information on the deployment, it is likely difficult for Congress to determine if FirstNet and AT&T are using the resources provided by Congress as intended, if the requirements in the law are being met, and if the network is being deployed as intended by Congress. Congress may request additional detail on FirstNet coverage, where the FirstNet network will be deployed and where it will not, and which regions will be served with persistent coverage versus deployable coverage.

Rural Coverage

The RFP required the inclusion of substantial rural coverage milestones with each phase of deployment, as required in the act. However, the contract allowed bidders to submit their own innovative solutions to meeting these requirements, and to set the base against which these milestones must be achieved. For example, within 12 months of award, the contract requires "Achievement of 20% of contractor's proposed Band 14 coverage in rural areas."[55] The contractor was permitted to set the base against which the milestones must be achieved. And, because the contract and the state deployment plans were deemed proprietary, the coverage offered by the contractor is not available for public view; as a result, there does not appear to be enough information to determine if the milestones are "substantial," as required under the act.

While the targeted milestones are a useful gauge for FirstNet to measure progress, the milestones are anchored to the contractor's proposed Band 14 coverage, which has been deemed proprietary and is not available for public view. Without knowing the nationwide Band 14 coverage offered by AT&T, it is difficult to assess the validity of contract milestones, as they are a percentage of an unknown factor. Further, due to the proprietary nature of the contract and the state plans, it is

[51] Sandra Wendelken, "AT&T Exec: FirstNet Contract Requires Undisclosed Number of Sites to Be Built," *Mission Critical*, December 12, 2017.https://www.rrmediagroup.com/Features/FeaturesDetails/FID/808, https://www.rrmediagroup.com/Features/FeaturesDetails/FID/808.

[52] FirstNet, "Nationwide Coverage," https://www.firstnet.com/coverage

[53] This may include cell-on-wheels (COW), cell-on-light-truck (COLT) or other deployable coverage options.

[54] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, Response to Questions for the Record submitted by Chris Sambar to Sen. Thune, 115th Cong., 1st sess., July 20, 2017, https://www.commerce.senate.gov/public/_cache/files/3c2c1b6b-8e2d-4275-a0a8-d09f534effbc/7A2F902BCF0DE992179D2AA6AB6ECE48.mr.-sambar-07.20.17-senate-cst-qfrs.pdf.

[55] Department of the Interior (on behalf of FirstNet), *FirstNet Nationwide Public Safety Broadband Network (NPSBN)*, Request for Proposal (RFP), Target Timeline, Herndon, VA, January 13, 2016, pp. Section J-8, https://www.fbo.gov/utils/view?id=bc4a63534ebd1fd64cd01ff070f25603.

difficult to determine which areas are included in the milestones (i.e., which areas will be covered) and which areas are not.

Congress may request more information on FirstNet coverage, rural milestones, and areas that will be covered under FirstNet, to determine if the "substantial rural coverage" requirements in the law are being met.

Rural Partnering Agreements

In the act Congress directed 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 deployment in rural areas." FirstNet included a 15% partnering requirement in the RFP, which AT&T has stated that it will likely exceed.

The Competitive Carriers Association (CCA)—which represents rural and regional carriers—expressed interest in partnering with FirstNet. In a November 2017 letter to Congress, CCA encouraged FirstNet to work collaboratively with all rural partners. CCA stated that rural and tribal telecommunication companies are often the only providers in rural regions, serve as the first line of defense in emergencies, and can provide reliable back-up during times of outages.

CCA noted that establishing partnerships would strengthen rural carriers and limiting partnerships could "delay and reduce services for public safety users, and result in AT&T using spectrum and funding provided by Congress for public safety use to eliminate commercial competitors."[56]

Due to the proprietary nature of the contract, information on the rural partnering agreements, which could indicate where rural coverage may be provided, is not available to the public. Congress may ask FirstNet where rural partnering agreements exist to ensure the requirement in the law concerning rural partnerships is met, and encourage FirstNet and AT&T to work with other interested partners and to expand service to rural regions.

Public Safety Grade

In the act, Congress requires the establishment of technical requirements to ensure the network is reliable, secure, resilient, and can withstand damage and disasters (e.g., hardening requirements). In 2013, FirstNet stated that the public safety broadband network will be "public safety grade" which, in simple terms, relates to standards by which public safety systems are built—with added requirements and features, to ensure the network keeps working in the harshest conditions, during emergencies and after. For example, public safety sites may have additional or extended back-up power, multiple paths to backhaul network traffic, and extensive site hardening to ensure communications systems are sustained during emergencies (e.g., tornados, earthquakes).

In a congressional hearing in July 2017, Senators raised questions regarding the reliability of the AT&T network, and whether the network was considered "public safety grade." In response, AT&T noted that there is variability in the definition of "public safety grade," and that its network is built to meet federal, state, and local laws, standards, and requirements. AT&T stated that its network is reliable, and when and if it experiences outages, AT&T has a robust deployable

[56] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Communications and Technology, *Oversight of FirstNet: State Perspectives*, Letter for the Record, submitted by the Competitive Carriers Association (CCA), 115th Cong., 1st sess., November 1, 2017, http://docs.house.gov/meetings/IF/IF16/20171101/106569/HHRG-115-IF16-20171101-SD004-U4.pdf.

solution (i.e., extensive portfolio of deployable assets, emergency operations center, and customer support) that can be used to restore the network, as demonstrated in the 2017 hurricane season.[57]

Although commercial systems meet all federal, state, and local siting, building and maintenance laws governing telecommunication systems, they do not always meet the higher-level standards for availability and reliability of public safety systems.[58] Congress may consider requesting more information on AT&T's network since it has been offered to public safety users while the FirstNet network is being built; Congress may seek to ensure the AT&T network being used by public safety is secure, reliable, resilient, and has redundancies built in to ensure that it will withstand major events (e.g., hurricanes, tornadoes), and that public safety communications are protected.

Further, Congress may consider requesting more information on how FirstNet and AT&T will ensure that the FirstNet network will be reliable and resilient, and able to withstand damage or disasters. The National Public Safety Telecommunications Council (NPSTC), in conjunction with public safety organizations and the standards development organizations, has released "Defining Public Safety Grade Systems and Facilities," which included input from multiple public safety organizations, best practices and requirements on network hardening and network reliability.[59] NPSTC acknowledged that it would be difficult and costly to implement all the best practices throughout a nationwide data system, on every site, but the report provided public safety network needs, and benchmarks for achieving a true "public safety grade" network.

Similarly, AT&T stated that, "We need a public-safety-grade network that extends from the handsets to the central office," however, given the resources, "[it's] not reasonable to think every tower will be at public-safety-grade level ... there needs to be some ranking …we are working with the states … and with the PSAPs (public-safety answering points)."[60] FirstNet and AT&T have stated that they will continue to work with states to identify critical assets that need to be hardened. Congress may seek to confirm that FirstNet and AT&T are adhering to the technical requirements established for the network under the law. Further, Congress may inquire how FirstNet/AT&T decides which sites are hardened, and how it expects future revenues will be used for public safety grade improvements.

The security, reliability, and resiliency of the FirstNet network are important to not only ensuring the network will continue to operate during and after major disasters, but also to gaining the buy-in of public safety users. In its July 2017 report, GAO noted that public safety stakeholders it interviewed raised concerns about several aspects of the network, including resiliency; reliability; redundancy; cybersecurity; frameworks for user identity, credentialing of users, and access management; and prioritization of users on the network. States raised similar concerns during the review of state plans.[61] Congress may consider requesting more information from FirstNet and AT&T on the FirstNet network's public safety grade features and when they will be available to public safety users, as these issues may affect state and local public safety agencies' decisions to

[57] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, 115th Cong., 1st sess., July 20, 2017, https://energycommerce.house.gov /hearings/oversight-firstnet-state-perspectives/.

[58] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Communications and Technology, *Oversight of FirstNet: State Perspectives*, 115th Cong., 1st sess., November 1, 2017.

[59] NPSTC, *Defining Public Safety Grade Systems and Facilities*, May 22, 2014, http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file= Public_Safety_Grade_Report_140522.pdf.

[60] Sandra Wendelken, "AT&T Exec Backtracks on Public Safety Grade Comments," *Mission Critical*, September 7, 2017, https://www.rrmediagroup.com/News/NewsDetails/NewsID/15933.

[61] See California's comments, requesting additional information on site hardening, http://www.caloes.ca.gov/PublicSafetyCommunicationsSite/Documents/FirstNetinCaliforniaStatePlanReviewResults.pdf, p.12.

join the network, the ability of the project to be self-sustaining, and the success of the network. Congress may also consider inviting state and local public safety users to testify at hearings on FirstNet to understand issues affecting subscribership.

Mission Critical Push-to-Talk (MCPTT)

Most public safety agencies use land mobile radios (LMR) to communicate. Commercial vendors have developed specialized features to meet the specific needs of public safety users during day-to-day operations and emergencies. Mission critical push-to-talk voice (MCPTT)[62] includes several features that have been standardized for LMR devices and systems, including:

- Direct Mode (i.e., allows device-to-device communication with nearby users off-network, when out of network range, or if the network is down);
- Push-to-Talk (PTT) (i.e., the responder pushes a button to talk, and releases the button to listen, which promotes ease of use);
- Group call (i.e., enables one-to-many communications);
- Full Duplex Voice (i.e., enables responders to communicate with parties outside their own PTT systems, including citizens with emergencies, and other agencies);
- Alerting (i.e., indicates a responder has encountered a life threatening emergency);
- Talker identification (i.e., similar to caller identification); and
- Audio Quality (i.e., high audio quality to enable the listener to better understand the speaker).

Public safety users want these features on the FirstNet (Band 14) network and devices. However, the standards for MCPTT features (e.g., direct mode, PTT, alerting) for LTE devices and networks (including FirstNet) were not yet developed when the law was signed.[63] 3GPP—the international standards development organization—prioritized the development of technical standards for public safety broadband and declared that establishing common technical standards for commercial cellular and public safety features will ensure interoperability between different vendors and lead to a competitive equipment market.[64]

The standards for MCPTT over LTE networks were recently approved by 3GPP, but still need to be tested and validated, which will take time. Therefore, at first launch, the FirstNet (Band 14) network will not offer MCPTT voice. Responders should be able to talk on FirstNet/AT&T devices, but the MCPTT features—critical features for first responders—will not be available on the FirstNet network. FirstNet has noted that the network will primarily be a high-speed *data* network. "The network is expected to initially transmit data, video, and other high-speed features, such as location information and streaming."[65] FirstNet has said that it is expecting to be able to offer MCPTT technology across the network by March 2019.

As a result, state and local public safety agencies may continue to use their LMR systems, until all features, including MCPTT voice, are available from FirstNet. The delay of MCPTT features

[62] NPSTC, *Mission Critical Voice Communications Requirements for Public Safety*, 2011 http://www.npstc.org/download.jsp?tableId=37&column=217&id=2055&file=Mission%20Critical%20Voice%20Fu.

[63] Dan Verton, "FirstNet Facing Commercial Device Reality, but Market and Security Concerns Persist," *fedscoop*, October 9, 2014, https://www.fedscoop.com/firstnet-facing-commercial-device-reality-but-security-concerns-persist/.

[64] See 3GPP webpage on Public Safety: http://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety.

[65] See FirstNet Network webpage: https://firstnet.gov/network/lmr.

may impact agencies' willingness to subscribe to the network, and affect FirstNet's ability to ensure the network is self-sustaining, as required under the law.

FirstNet has begun to offer devices that will be able to operate on the FirstNet network, with modified features for public safety (e.g., proprietary push-to-talk, ruggedized devices). However, questions have been raised about these devices and the device policy.

Some Members of the House Energy and Commerce Committee raised questions regarding whether FirstNet devices can successfully roam onto rural wireless networks. AT&T confirmed that responders will be able to roam across various networks because they all operate on 3GPP standards. However, it is not clear if FirstNet users can roam on *all* rural networks, or just those carriers that have agreements with AT&T.

Some carriers have raised questions on device interoperability. The Competitive Carriers Association (CCA) asserts that the AT&T devices are "compatible only with AT&T's boutique Band Class 17 ... and may not be compatible with the public safety spectrum in Band Class 14, [and] ... unable to access a connection in areas outside of AT&T's commercial network."[66]

Public safety advocates have raised questions on whether other carriers that install Band 14 into their devices would be able to access FirstNet services.[67] It is not clear if users would have to pay for two subscriptions—one for the primary carrier, and another to FirstNet; or if non-AT&T device-holders would be able to roam onto all of AT&T bands or just Band 14, which could affect the ability of agencies to interoperate.

At a June 2017 hearing, witnesses testified on the number of responders that use their own personal devices for work, such as volunteer firefighters.[68] FirstNet/AT&T stated it would establish a Bring Your Own Device (BYOD) policy for those users, and that it would certify personal devices for compatibility, interoperability, and security.

FirstNet is working to expedite the development of LTE Band 14 devices, and has testified that it supports the development of standards-based, non-proprietary devices, equipment, and applications that will be interoperable across various networks. FirstNet is facilitating the testing of devices at its Innovation Lab in Boulder, CO, and it is playing an active role in standards-development, as required under the act. In 2017, FirstNet attended Mobile World Congress, where they arranged market research meetings with LTE device vendors to discuss the optimum integration of LTE Band 14 within their products and to promote key public safety features such as Proximity Services (ProSe), direct device-to-device communications, and MCPTT standards.[69]

Congress may continue monitoring progress of FirstNet devices to ensure that devices, and features on those devices, are standards-based and interoperable. Further, Congress may consider allowing the flexible use of federal grant funds for multiple technologies (e.g., LMR, LTE, dual-

[66] U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Communications and Technology, *Oversight of FirstNet: State Perspectives*, Letter for the Record, submitted by the Competitive Carriers Association (CCA), 115th Cong., 1st sess., November 1, 2017, http://docs.house.gov/meetings/IF/IF16/20171101/106569/HHRG-115-IF16-20171101-SD004-U4.pdf.

[67] Andrew Seybold, "Public Safety Advocate: FirstNet or SecondNet?" *All Things FirstNet*, August 17, 2017, http://allthingsfirstnet.com/public-safety-advocate-firstnet-or-secondnet/.

[68] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, Testimony by Dr. Damon Darsey, 115th Cong., 1st sess., July 20, 2017, https://www.commerce.senate.gov/public/_cache/files/1dcae52b-4f87-427b-a57a-d6541f680230/62666C224843330B4332AF4E21A45C85.darsey-testimony.pdf.

[69] FirstNet Blog, *FirstNet Tech Team Goes to 2017 Mobile World Congress*, https://www.firstnet.gov/newsroom/blog/firstnet-tech-team-goes-2017-mobile-world-congress.

use) to allow interoperability across systems (e.g., FirstNet and LMR systems), and to allow public safety agencies flexibility to transition to FirstNet as they are able.

Cybersecurity

The act requires that the network be safe, secure and reliable, and have protections in place against cyber attacks. FirstNet/AT&T leveraged industry best practices and federal best practices to ensure a secure network for public safety.[70]

AT&T plans to integrate cybersecurity into devices and applications. All devices are to be screened before users can access the network; AT&T plans to screen devices based on AT&T standards; then FirstNet plans to screen devices, based on the federal standards encompassed in the NIST Cyber Security Framework.[71] FirstNet/AT&T plans to provide a highly secure Identify Management and Federated Credential and Access Management system (ICAM)[72] that enables a secure, single sign-on for FirstNet users. FirstNet is working with the Departments of Homeland Security, Justice, and Commerce and the Office of Management and Budget to leverage cyber best practices and to ensure the network is secure.[73]

FirstNet is to be built with layers of security, designed into RANs, the core network, and service platforms, as well as the devices. Firewalls are to enforce stringent security policies developed in cooperation with DHS and Department of Defense (DoD) to meet NIST requirements. The FirstNet design is to be guided by 3GPP standards for encryption and other standards-based security measures and best practices. Communications is to run on a separate core that is both wireless and encrypted, to ensure public safety communications are secure. Further, AT&T is to provide an operations center to monitor traffic on the FirstNet network and ensure it is secure.

Despite these activities, there are cybersecurity risks. Applications developed for the network by outside developers will need to be screened and secure. A 2017 pilot project conducted by the DHS Science and Technology (S&T) Directorate found that 33 popular apps used by public safety had security and privacy concerns; DHS emphasized the need to screen and test public safety apps for vulnerabilities.[74]

In its July 2017 report, GAO reported that a local government official expressed uncertainty with the security of the FirstNet network, noting that having a large concentration of sensitive public-safety information traveling through one network may be viewed as a target for cyber attacks.[75] The President's National Security Strategy noted the same risk, and emphasized the need to

[70] National Association of State Chief Information Officers (NASCIO), "NASCIO Response to Appendix C-10: NPSBN Cybersecurity," 2015, https://www.nascio.org/Portals/0/Advocacy/2015/SpecialNotice-CyberRESPONSE-%20Final.pdf.

[71] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework.

[72] ICAM webpage on FirstNet.com, https://www.firstnet.com/power-of-firstnet/value-of-firstnet/identity-control.

[73] Meredith Somers, "FirstNet Teams Triage Cyber Security, Rural Coverage as They Build Out Network," *Federal News Radio,* July 20, 2017, https://federalnewsradio.com/technology-main/2017/07/firstnet-teams-triage-cybersecurity-rural-coverage-as-they-build-out-first-responder-network/.

[74] DHS Science and Technology, "DHS S&T Pilot Project Helps Secure First Responder Apps from Cyber Attacks," press release, December 18, 2017, https://www.dhs.gov/science-and-technology/news/2017/12/18/news-release-st-pilot-project-helps-secure-first-responder.

[75] U.S. Government Accountability Office, Public-Safety Broadband Network: FirstNet Has Made Progress Establishing the Network, but Should Address Stakeholder Concerns and Workforce Planning, GAO-17-569, June 2017, https://www.gao.gov/assets/690/685327.pdf.

prioritize U.S. efforts, capabilities, and defenses where cyber attacks could have catastrophic or cascading consequences, including networks used for national security and public safety. [76]

To ensure the network is secure, as required under the act, Congress may encourage FirstNet to continue to engage with federal partners, and state and local Chief Information Officers (CIO), to ensure cybersecurity policies are in place and enforced. Congress may encourage training on cyber risks for FirstNet users, and information-sharing on cyber incidents.

Applications

Under the act, the FirstNet network was required to evolve as new technologies developed. Bidders to the RFP were required to provide an application ecosystem that supports the nationwide public safety broadband network with services relevant to public safety.[77]

For the past several years, FirstNet has engaged in outreach to public safety to collect input from first responders on useful data applications, and mobile broadband tools and technologies that could save lives. For example, FirstNet allows developers and/or first responders to test apps through the FirstNet lab, and to provide input on new applications.

Both the network and applications on the network need to be interoperable to ensure a consistent user experience, and to ensure features offered through the network do not hinder interoperability. Further, applications developed for FirstNet need to be secure. Applications developed by outside developers could introduce malware, viruses, or other cybersecurity risks to the network. Congress can encourage FirstNet to continue to work with federal agency partners (e.g., DHS, NIST) who bring expertise in cybersecurity, to ensure FirstNet applications are secure, and will not pose a risk to the public safety network or to other federal systems. Continual collaboration with federal partners on applications will likely help to ensure that FirstNet applications are secure, interoperable, and will serve future federal users.

Innovation

FirstNet has spurred innovation in public safety communications, providing mobile broadband devices and solutions, innovative applications, and creating opportunities to move public safety toward 5G technologies. Under the Public Safety Innovation Accelerator Program, FirstNet and NIST are conducting public safety broadband research. This program received $300 million under the act to fund research and development in public safety broadband; $38.5 million has been awarded to conduct research on improving resiliency, real-time video analytics, location-based services for public safety, mission critical push-to-talk technologies, and improving indoor communications.[78] Looking ahead, there are three issues of concern:

- It is not clear how the costs of upgrades (to 5G) will be shared between FirstNet/AT&T and state and local public safety agencies. Not all agencies may be able to afford advanced technologies, creating gaps in capabilities across users of the network.

[76] U.S. President (Trump), "National Security Strategy of the U.S.," https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[77] Applications are software programs that run on computers. Each program has a specific "application" for the user, such as fleet management, incident management, management of devices and security settings on devices, cloud storage options. The FirstNet RFP required the development of a broad applications ecosystem for public safety users.

[78] NIST, "NIST Awards $38.5 Million to Accelerate Public Safety Communications Technologies," June 13, 2017, https://www.nist.gov/news-events/news/2017/06/nist-awards-385-million-accelerate-public-safety-communications.

- State and local entities are beginning to address privacy concerns related to video cameras and drones, and jurisdictional concerns related to the siting of small-cell equipment.[79] FirstNet established recommended security and privacy specifications for mobile and Internet of Things (IoT) devices (e.g., traffic cameras, monitoring systems for buildings, sensors which could feed information back to public safety officials through the FirstNet network).[80] While these security and privacy specifications may help to address public concerns about these new technologies, they may not be consistent with state and local laws.
- State and local entities will need to update communication governance bodies, standard operating procedures, training, and exercises to integrate FirstNet technologies into response protocols. Including Chief Information Officers (OCIO) may help with integration of FirstNet technologies and cybersecurity.

Congress may seek to expand eligible activities and allowable costs in federal grants, to enable public safety users, including responders from smaller localities and volunteer responders, to access the advanced technologies offered through FirstNet and AT&T, and to encourage state and local investment in activities that help to integrate FirstNet capabilities into response plans, procedures, training, and exercises.

Affordability and Sustainment

Under the act, the network must be permanently self-funded. The GAO has stated that FirstNet/AT&T have established a framework to finance the network to meet that requirement.

FirstNet/AT&T can charge users (e.g., public safety users, secondary users) for their use of the FirstNet network. AT&T can also monetize (i.e., earn revenue from) the excess capacity of FirstNet's 20 MHz of broadband spectrum, when it is not in use by public safety.

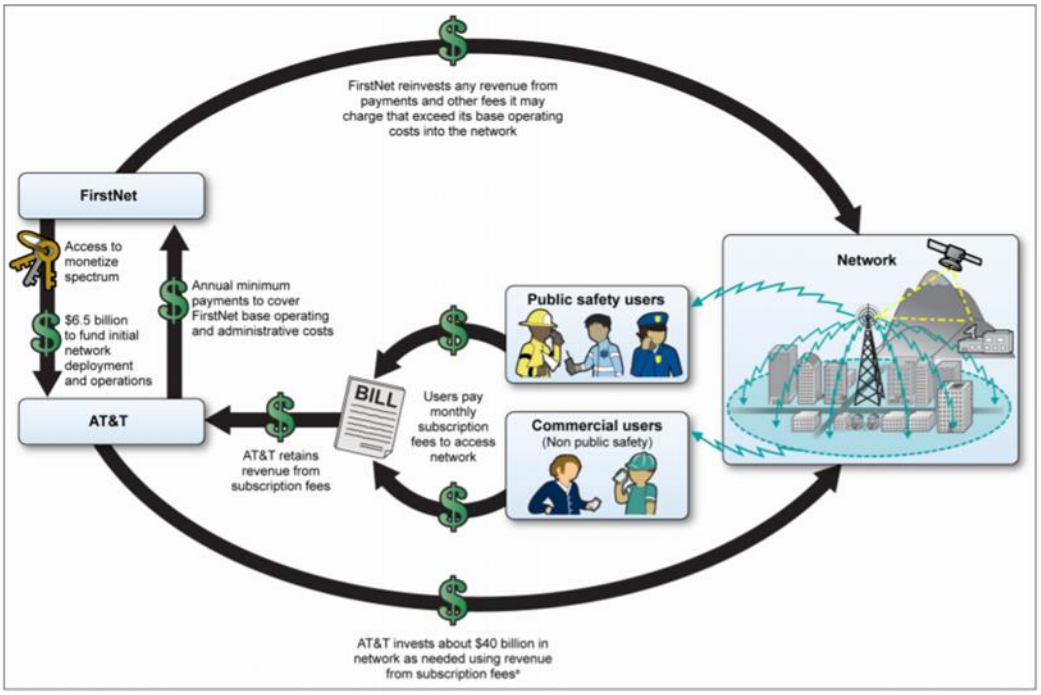
From this revenue, AT&T must pay (a) FirstNet operating and administrative fees, and has committed (b) $40 billion over the life of the contract to support the build-out, operation, and maintenance of the FirstNet network.[81] **Figure 3** provides a graphic of the funding model, as depicted by GAO.

[79] CRS Report R42543, *The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress*, by Lennard G. Kruger.

[80] Darnell Washington, "First Responders: The Key to Wireless Security?" *Security InfoWatch*, October 16, 2017, http://www.securityinfowatch.com/article/12369845/first-responders-the-key-to-wireless-security.

[81] AT&T Corporate webpage on AT&T Public Safety Solutions, https://www.corp.att.com/public-safety/.

Figure 3. FirstNet Financial Framework



Source: GAO-17-569 U.S. Government Accountability Office, Public-Safety Broadband Network: FirstNet Has Made Progress Establishing the Network, but Should Address Stakeholder Concerns and Workforce Planning, GAO-17-569, June 2017, https://www.gao.gov/assets/690/685327.pdf.

While the act required states to either opt-in or opt-out of deploying the RAN in their state, it did *not* require public safety agencies to subscribe to FirstNet. Even if a state opted into the network (i.e., opted to have FirstNet/AT&T deploy the network in their state), the public safety agencies in the states are not required to subscribe to the network. Agencies can continue to use their existing LMR systems, current commercial cellular/broadband providers, or both.

A financial challenge for FirstNet/AT&T will be in enrolling subscribers to the system. Likely, FirstNet/AT&T must offer better coverage, services, and features than they currently have, at a price public safety agencies can afford, if they want to attract users to the network. Users will need to weigh the cost of new equipment and new devices, and the cost of the subscription (including any add-on costs for specialized public safety services) in their decision to subscribe.[82]

There are three issues for congressional consideration:

(1) FirstNet/AT&T have focused on primary users (e.g., state, local, territory, tribal public safety entities) over the past three years. Congress may ask FirstNet/AT&T about their progress in attracting other users (e.g., federal agencies, 9-1-1 centers, telemedicine providers), to increase subscribers, and to encourage interoperability between agencies, as intended under the law.

(2) Many public safety users have stated that they will continue to support LMR (radio) systems for mission critical voice, even if they transition to FirstNet, to ensure first responders always have access to mission critical voice, as primary communications or as back-up communications. User fees for LMR systems have not been able to sufficiently fund state and local LMR

[82] See California discussion regarding added fees for use of application to access CJIS: https://blog.npstc.org/2018/01/03/californias-firstnet-complaints-highlight-build-out-adoption-challenges/.

systems;[83] adding additional user fees for FirstNet may present financial challenges for state and local agencies.

(3) Regional partnerships, added funding streams, and joint purchasing agreements have helped to support LMR systems.[84] Congress may seek to encourage states to develop financial models to support both LMR and FirstNet services. Congress may consider allowing the flexible use of grant funds to enable state and local agencies to fund LMR systems and FirstNet expenses, including devices and activities that integrate FirstNet capabilities into response, including governance, planning, protocols, training, and exercises. The flexible use of federal grant funds will allow public safety agencies to transition to FirstNet when they are financially and operationally ready.

Conclusion

To ensure the $6.5 billion federal funding and 20 MHz of public safety spectrum provided for this project is used to benefit public safety, Congress can monitor the deployment and use of the network over time. Congress may continue oversight of the FirstNet network to better understand the deployment and critical aspects of the network; to ensure that the network is being deployed as intended by Congress; and to ensure that public safety users are subscribing to the network, which is needed to support current operations and future improvements to the network. Congress may include public safety stakeholders in hearings on FirstNet, to ensure that public safety needs (e.g., coverage, resiliency, security) are met and that the network is available, affordable, and sustainable for all users. Congress may inquire about FirstNet's staffing to ensure FirstNet has adequate staff to manage the contract, oversee the deployment, and assist users, as recommended by the GAO.

Lastly, Congress and public safety have long recognized that technology is not the sole driver of an effective response. Congress may seek to encourage state and local agencies to integrate FirstNet capabilities into response plans, protocols, training, and exercises, to ensure that public safety agencies are ready to leverage FirstNet technologies when the next emergency strikes.

[83] State of Minnesota, *Minnesota—Arner and 9-1-1 Funding Study*, February 2014, p. 18, https://dps.mn.gov/divisions/ecn/programs/armer/Documents/minnesota-armer-and-ng911-funding-study.pdf.

[84] DHS Office of Emergency Communications, *Funding Public Safety Communication Systems*, 2015, https://www.dhs.gov/sites/default/files/publications/Funding%20Mechanisms_TechEdit_11202015_1.pdf.

Appendix A. Related Issues in the Act

9-1-1 Improvements

The act authorized $115 million for a grant program to upgrade public safety answering points (PSAPs) to NG911 capabilities. The NG911 grant program is to provide financial assistance to PSAPs to help fund the establishment of IP-based backbone networks, the application layer software infrastructure needed to interconnect a multitude of response organizations, trainers, call-takers and first responders.

NTIA and NHTSA finalized a management plan to jointly administer the grant and submitted that plan to Congress in January 2017.[85] In September 2017, the NTIA and NHTSA released draft program requirements in the *Federal Register*,[86] seeking comment on the grant. This $115 million grant is to enable some PSAPs to upgrade their networks, but not all PSAPs are to receive funding. Congress can monitor the grant terms and formulas, to ensure that funding is used wisely, and that underserved PSAPs are encouraged to apply.

Congress may seek to ensure that FirstNet and the 911 community engage early, before the deployment of the Band 14 network, to ensure that 911 needs are considered in the earliest stages of network planning and deployment. Congress can encourage FirstNet/AT&T to work in tandem with the 911 community to ensure that upgrades planned for both systems are coordinated, and to ensure that PSAPs can be integrated into the FirstNet network, as encouraged in the act.[87]

Spectrum Relocation: T-Band

In the same act that created FirstNet, Congress directed the FCC to reallocate the spectrum in the 470-512 MHz band (also known as the T-Band spectrum) from public safety to commercial use. This spectrum is currently used by 925 public safety licensees in eleven metropolitan areas, for land mobile radio (voice) communications.[88]

The act requires that, within nine years of enactment (i.e., by February 22, 2021), the FCC must reallocate the T-Band public safety spectrum and begin the auction process. Two years after the bidding is complete (~2023), relocation of T-Band public safety entities is required to be completed. NTIA is required to use the proceeds from the bidding process to make grants to cover relocation costs of those public safety entities from the T-Band spectrum.[89]

Public safety advocates believe that Congress saw two options for T-Band operators: relocate those agencies to other frequencies in the area; or, migrate those agencies to the FirstNet network, once it is operational.

---

[85] NHTSA and NTIA, *Management Plan for the Next Generation 9-1-1 Grant Program,* https://www.ntia.doc.gov/files/ntia/ publications/nhtsa_ntia_ng911_grant_program_management_plan.pdf.

[86] NHTSA and NTIA, "911 Grant Program," 82 *Federal Register* 44131, September 21, 2017, https://www.federalregister.gov/documents/2017/09/21/2017-19944/911-grant-program.

[87] During 9/11, 9-1-1 call-takers had no information about the impact zone and so were unable to provide informed instructions to callers. The 9/11 Commission, *The 9/11 Commission Report*, July 22, 2004, p. 286, https://www.9-11commission.gov/report/911Report.pdf.

[88] Including Boston, MA; Chicago, IL; Dallas/Ft. Worth, TX; Houston, TX; Los Angeles, CA; Miami, FL; New York, NY/Northern NJ; Philadelphia, PA; Pittsburgh, PA; San Francisco/Oakland, CA; Washington, DC/MD/VA.

[89] Section 6103 (b) of P.L. 112-96.

Public safety agencies operating on the T-Band argue that there are no frequencies available in the area, which is why they were operating on the T-Band originally. In 2013, NPSTC conducted a study of spectrum and options available to T-Band licensees. The study confirmed probable shortages in several regions, and significant shortages in the five largest urban areas.[90] Further, NPSTC estimated the cost of transition at approximately $5.9 billion, and raised questions as to whether the auction, as it is structured, would be able to attract bidders.[91]

In October 2014, the FCC offered the 700 MHz narrowband reserve channels for general licensing and afforded T-Band public safety licensees priority access to these channels in the T-Band areas.[92] NPSTC issued a *T-Band Update Report* in May 2016, concluding: "Although these 24 additional 700 MHz band channels are certainly beneficial, the number of additional channels pales in comparison to the T-Band channels in use that would need to be relocated to alternative spectrum, especially in the top five T-Band areas."[93]

The second option for T-Band operators suggests agencies could migrate to the FirstNet network. Public safety agencies have argued that this is not a viable option, because FirstNet will not offer mission-critical voice at first launch, which would negatively affect response in those regions.

At a November 1, 2017 hearing of the House Committee on Energy and Commerce, Subcommittee on Communications and Technology, Congress emphasized that it does not want to disrupt critical communications capabilities or lose mission critical voice capabilities during the deployment of the FirstNet network. [94] FirstNet reported that the standards process for MCPTT is proceeding, and it is eager to provide MCPTT to FirstNet primary users. However, the critical factor is time. At its June 2017 Board meeting, FirstNet staff presented board members with a roadmap that includes an update on the standards development process. FirstNet provided a commitment to support MCPTT across the nationwide network by 2019, which brings T-Band agencies closer to the statutory deadline for relocation (~2023) and does not leave a lot of time to transition systems and train people. [95]

The agencies affected by this issue are all located in large population centers. The systems affected by this policy are public safety systems, protecting the life and property in these regions, including the lives of first responders. Congress may consult with affected jurisdictions/agencies to understand the impact of T-Band migration on public safety communications, and to consult with the FCC on relocation options and timelines.

[90] Boston, Chicago, Los Angeles, New York, and Philadelphia.

[91] NPSTC, *T-Band Update Report*, May 31, 2016, p. 31, http://www.npstc.org/download.jsp?tableId=37&column=217&id=3696&file=T_Band_Update_%20Report_Final.pdf.

[92] FirstNet, T-Band Fact Sheet, https://www.firstnet.gov/sites/default/files/T-Band_FactSheet_July2016_0.pdf.

[93] NPSTC, *T-Band Update Report*, May 31, 2016, p. 31, http://www.npstc.org/download.jsp?tableId=37&column=217&id=3696&file=T_Band_Update_%20Report_Final.pdf.

[94] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Communications, Technology, Innovation, and the Internet, *An Update on FirstNet*, 115th Cong., 1st sess., July 20, 2017; and U.S. Congress, Senate Committee on Commerce, Science, and Transportation, Communications, Technology, Innovation, and the Internet, *Oversight of FirstNet: State Perspectives*, 115th Cong., 1st sess., November 1, 2017. https://energycommerce.house.gov/hearings/oversight-firstnet-state-perspectives/.

[95] FirstNet Board Minutes, June 28, https://www.firstnet.gov/sites/default/files/Board%20Committee%20Meeting%20June%202017%20.pdf.

Appendix B. Related Legislation

Don't Break Up the T-Band Act (H.R. 5085)

Section 6103 of P.L. 112-96 requires public safety agencies to "give back" their T-Band spectrum by 2023. The T-Band (470-512 MHz) is used by public safety agencies in 11 metropolitan regions, for public safety communications. Public safety agencies have argued that there is not sufficient or comparable spectrum for them to migrate, and that the migration would disrupt public safety communications in these populous regions. In February 2018, Representatives Engel, Zeldin, and King of New York introduced the Don't Break Up the T-Band Act of 2018 which calls for the repeal of Section 6103 of P.L. 112-96.

Internet of Things Cybersecurity Improvement Act of 2017 (S. 1691)

In August 2017, Senators Warner, Garner, Wyden, and Daines introduced the Internet of Things (IoT) Act which provides minimum cybersecurity standards for internet-connected devices purchased by federal agencies. This act would direct the Office of Management and Budget (OMB) Director to work with the DoD, General Services Administration (GSA), Department of Commerce, and DHS to issue guidelines for executive agencies to include certain language in contracts for the acquisition of internet-connected devices. This bill would require contractors to certify that hardware, software, or firmware does not have any known vulnerabilities or security defects, to protect federal IT systems. "Under the terms of the bill, vendors who supply the U.S. government with IoT devices would have to ensure that their devices are patchable, do not include hard-coded passwords that can't be changed, and are free of known security vulnerabilities, among other basic requirements."[96] The bill also would require executive agencies to inventory all internet-connected devices in use by the agency, and to create standards for purchases to protect federal systems from malicious attacks. FirstNet and AT&T are already discussing the potential intersection of IoT and public safety (e.g., location data from third-party sources, sensors to monitor infrastructure, video systems to increase situational awareness).

NG911 Act (S. 2061)

In March 2017, Senators Nelson and Klobuchar introduced the NG911 Act which would accelerate the deployment of NG911 services. The NG911 bill would expand a federal grant program to support NG911 improvements. The bill would support standards-based purchases and promote interoperability with FirstNet.

Further, the bill would expand the definition of NG911 to include multiple technologies and multiple means of contacting 9-1-1 (e.g., call, text). This act would also require NIST to prepare a report on NG911 cyber vulnerabilities, the FCC to prepare a report to determine whether agencies are following 9-1-1 best practices, and the GAO to prepare a report on PSAP resiliency and how that can be improved.

[96] Senator Mark R. Warner, "Senators Introduce BiPartisan Legislation to Improve Cybersecurity of Internet of Things" (IoT) Devices," press release, August 1, 2017, https://www.warner.senate.gov/public/index.cfm/2017/8/senators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices.

Author Contact Information

Jill C. Gallagher
Analyst in Telecommunications Policy
jgallagher@crs.loc.gov, 7-1024