Homeland Security
Science and Technology

TechNote

U.S. Department of Homeland Security

SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?" These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. This TechNote was prepared for the SAVER Program by the Space and Naval Warfare Systems Center Atlantic.

SPAWAR Systems Center ATLANTIC

For more information on this and other technologies, contact the SAVER Program by e-mail or visit the SAVER website.

E-mail: saver@hq.dhs.gov
Website: www.firstresponder.gov/SAVER

FirstNet: Building a Nationwide Public Safety Broadband Network

When responding to a national disaster, such as Hurricane Katrina, or a major incident, such as the Boston Marathon bombing, emergency responders rely on their communication devices to coordinate responses with other emergency responders. Often, communications are hindered because the cellular network is unavailable due to power or equipment failures, the network is overloaded with traffic, and/or emergency responders are responding in an area with limited or no network coverage. In addition, communications are further hindered due to multiple agencies and/or jurisdictions operating their devices on different frequencies. To address these issues and improve emergency responders' ability to respond to incidents, a nationwide wireless broadband network dedicated solely to their use is in development. First Responder Network Authority (FirstNet) is expected to provide emergency responders with a reliable, secure network that facilitates real-time data communications among emergency responders throughout every state, territory, and tribal land.

Overview

Established by the Middle Class Tax Relief and Job Creation Act of 2012, the FirstNet is responsible for building the first wireless broadband network for public safety. This network will support mission-critical voice and data communications for emergency responders. When it is launched, users will be able to send data, video, and text messages over the network, with additional capabilities, such as location information and streaming video, coming online at a later date. Land mobile radio (LMR) networks will be utilized in the beginning for voice communications and eventually, FirstNet plans to utilize Voice over Long Term Evolution (VoLTE) for voice communications.

Network Architecture

The nationwide public safety broadband network (NPSBN) will be based on LTE technology and occupy the public safety section of the 700 MHz wireless spectrum (Band Class 14). The components of the network will include: a core network, transport backhaul, radio access networks (RANs), and public safety devices. The core network will process, store, and secure data; host applications and services; and interface with other state, local, and federal networks, including 911. The core will be connected to RANs by the transport backhaul component (i.e., fiber optics, coaxial cable). The RANs consist of infrastructure, such as cellular towers and mobile hotspots, which connect to public safety devices such as smartphones, laptops, tablets, and air cards.

Path Forward

In developing the NPSBN, FirstNet will partner with industry through a Request for Proposal (RFP) process to construct, operate, and maintain the network (Figure 1). In addition, FirstNet will consult with the states and territories on developing a plan for connecting to the network. Once the RFP and state consultation processes are complete, FirstNet will present a plan to each state. Each state will have the option of opting in or out of the network. If a state opts out, it has 180 days to submit an alternate plan to the Federal Communications Commission (FCC), who will approve or reject the plan. If the plan is rejected, the plan initially put forward by FirstNet will be implemented. Once the state plans have been finalized, FirstNet will begin building the network; the network is expected to be operational in 2022.

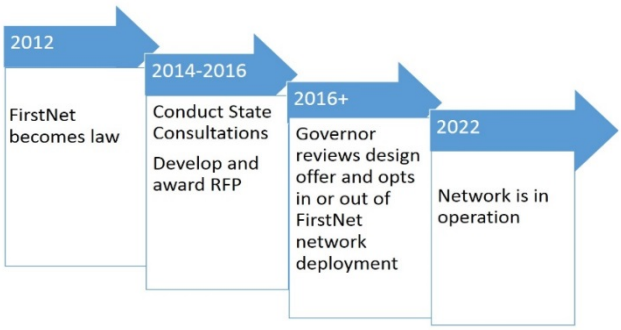

Figure 1. FirstNet Timeline

Implementation Considerations

A number of factors must be considered when building, deploying, and operating an NPSBN that provides reliable, secure coverage to rural and urban environments.

Public Safety Devices: A new class of smartphones and other devices to be used on the network will be required. Most smartphones used by emergency responders are not compatible with the public safety Band Class 14 spectrum. While some manufacturers are developing Band Class 14 compatible smartphones, many manufacturers are concerned about the costs associated with developing new products given the relatively small customer base. In an effort to keep costs down, FirstNet is exploring incorporating the necessary technology in existing, popular smartphones; however, this raises concerns about possible compromises to the network by hackers.

Coverage: The majority of U.S. land is considered rural or wilderness with limited to no network coverage. In addition, network coverage in urban environments can be limited or weakened due to factors such as proximity to a cellular tower or a building's composition when a user is indoors. To overcome these challenges, FirstNet plans to utilize land-based, satellite, and mobile-deployable systems to ensure network coverage in all areas and will try to leverage commercial wireless service providers' existing telecommunications infrastructures when possible.

Network Security: All layers of the network will need to be protected from cyber security threats. FirstNet will implement security measures and policies based on industry standards and best practices, including 3rd Generation Partnership Project (3GPP) standards and National Institute of Standards and Technology (NIST) standards.

Network Reliability: Cellular towers, backhaul technology, and other physical components of the network will need to be resilient to the environmental conditions in which they are located. This will require FirstNet to customize its hardening techniques since different regions in the United States are prone to different weather events (e.g., hurricanes, earthquakes, tornadoes). In addition, the network will need to build in redundancy to remain operational during power outages, equipment failures, and periods of high demand. For example, back-up power sources and diverse routing of network traffic are measures FirstNet will incorporate into the network.

Regulatory Compliance: Before FirstNet can begin building the network, it must determine compliance with environmental and historic preservations laws such as the National Environment Policy Act (NEPA) and National Historic Preservation Act (NHPA). To mitigate the time investment needed once plans are finalized, FirstNet is preparing five Programmatic Environmental Impact Statements (PEISs), which aim to address and mitigate potential environmental and historic issues associated with implementing the network.

Funding: Revenue streams for the capital and ongoing costs associated with building, deploying, operating, and maintaining the network are variables. While $7 billion in funding is expected to be made available through proceeds from spectrum auctions conducted by the FCC, the actual costs to create the network infrastructure and amounts to be raised remain undetermined. To minimize costs and accelerate development of the network, FirstNet is exploring public/private partnerships with major commercial wireless service providers to leverage their existing infrastructure. The fees that FirstNet will charge to agencies who utilize the network's services and devices are another unknown. FirstNet will develop a pricing model mindful of the need to price services to attract users while at the same time ensuring recurring costs will be covered.

For additional information and updates on the project's status, visit the FirstNet website at www.firstnet.gov.