Appendix B – Technology and Equipment Standards and Resources

This appendix provides grant recipients with operational best practices, technical standards, and resources to reference when developing communications systems. Above all, grant recipients should purchase standards-based technologies and equipment that promote interoperability with partners.

How to Use this Appendix

When procuring communications infrastructure, there are overarching considerations and guidelines, as well as specific standards to follow. No single document could include everything public safety communications system planners need to know. However, this appendix lists technical standards applicable to public safety communications systems and resources for additional information. The following topics are included in this appendix:

System Lifecycle Planning

Grant recipients should employ best practices and recommendations from the *2018 Emergency Communications System Lifecycle Planning Guide*

The Department of Homeland Security (DHS) Office of Emergency Communications (OEC), in collaboration with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), developed the *2018 Emergency Communications System Lifecycle Planning Guide*, which provides recommended actions through easy-to-use checklists for each phase of the system lifecycle planning model. It is intended for stakeholders to use in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually replace and dispose of system components.

Each phase of the system lifecycle planning model—Pre-Planning; Project Planning; Request for Proposals and Acquisition; Implementation; Support, Maintenance, and Sustainment; End-of-Lifecycle Assessment and Replacement; and Disposition—includes best practices, considerations, and recommended checklists to assist public safety agencies embarking on system lifecycle planning. Specifically, the checklists are designed to be torn-out, referenced, and used by project management teams throughout the system lifecycle. Table B-1 summarizes the system lifecycle planning model phases and high-level recommendations contained in the *2018 Emergency Communications System Lifecycle Planning Guide*. Reference the guide for additional information on recommendations.

Table B-1. System Lifecycle Planning Model and Recommendations Summary

Planning Model	Recommendations
Phase 1: Pre-Planning **Timing:** 6–12 months **Goals:** Inform and secure the decision to replace, upgrade, maintain, dispose of, and/or acquire a new system	• Establish the core planning team • Research and develop system and funding options • Decide on the optimal and alternative solutions with funding options • Plan for frequency needs and channel programming • Develop a business case, presentation materials, and strategic plan • Identify a legislative- or executive-level project champion • Present to decision-makers and secure funding to support the initial build-out and sustain the system throughout the entire lifecycle
Phase 2: Project Planning **Timing:** 6–18 months **Goals:** Formalize the project team; identify operational and technical requirements for system replacement and upgrade; and develop the project plan	• Consider how long the planning process can take and communicate expected timeframes to elected officials • Collect user needs and requirements and incorporate into project plans • Engage with communications leaders early for guidance and support (e.g., Statewide Interoperability Coordinators [SWIC], Statewide Interoperability Governing Bodies [SIGB]) • Identify strong Project Sponsors (e.g., state or local elected officials) • Begin planning the Request for Proposals (RFP)
Phase 3: RFP and Acquisition **Timing:** 6–12 months **Goals:** Select the appropriate procurement vehicle and procure systems and components	• Develop a written action plan • Form the RFP team • Develop the Statement of Work (SOW) • Include specifications or requirements in the RFP • Establish written evaluation criteria, well before the award • Conduct a formal objective review process and document results
Phase 4: Implementation **Timing:** 12–18 months **Goals:** Develop an implementation plan; install new systems; test; train users; and transition from legacy to new	• Develop the implementation plan • Understand and document testing procedures (e.g., factory testing, staging, site installation and testing, coverage verification, testing and acceptance, cut-over, final acceptance) • Update operational procedures and train users • Promote new communications capabilities and benefits to the community
Phase 5: Support, Maintenance and Sustainment **Timing:** Year(s) 1–25 **Goals:** Inventory and maintain equipment; manage budget; assess and communicate needs	• Maintain an accurate inventory of equipment (e.g., scope, database tool, inventory team, processes to compile and secure data) • Determine and execute an ongoing maintenance and operations model • Manage the budget when the project is conceived, directly before it is funded and after delivery • Share communications needs with decision-makers early and continually
Phase 6: End-of-Lifecycle Assessment and Replacement **Timing:** Years 7–25 **Goals:** Determine when to replace systems or components with solutions to best fit operational and technical needs	• Conduct ongoing assessments of current system (e.g., implement a balanced scorecard) to plan for technology maturity • Refresh or upgrade systems, as needed, to extend the life • Determine potential replacement solutions, with consideration to support national, state, and regional interoperability initiatives; consider early adoption of new technologies; and, adhere to widely-used technical standards
Phase 7: Disposition **Timing:** 90 days after cut-over or transition **Goals:** Determine options and dispose of legacy systems or components	• Develop the disposition plan • Determine options (e.g., reuse or repurpose old components, consider space availability, convey surplus equipment to partner agencies) in consideration of legal or policy limitations, and business requirements • Brief leaders on disposition plans • Identify lessons learned following disposition

Cybersecurity	Grant recipients should implement the *NIST Cybersecurity Framework*, consider participating in the C³VP, and use existing cybersecurity standards

Land mobile radio (LMR) has long been used by emergency first responders for mission critical communications. As technologies evolve, LMR systems are exposed to greater security risks such as jamming, eavesdropping, and denial of service. In addition, the emergency response community is deploying advanced voice, video, and data services over Internet Protocol (IP)-based networks to enhance response operations. Although these services enhance capabilities, they also introduce new and significant cyber risks that the emergency response community must plan and address. Traditional emergency communications systems have limited means of cyber entry, but IP-based platforms enable interconnection with a wide range of public and private networks, such as wireless networks and the Internet.

The public safety community must continually identify risks and address evolving security requirements. Emergency communications cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, and even the public. To protect emergency communications from cyber threats and attacks, recipients will need to invest in solutions that enhance cybersecurity posture. Cybersecurity must be addressed through planning, governance, and technology solutions that secure networks. Recipients should ensure cybersecurity planning is comprehensive and addresses all network component lifecycles, and updates to non-technology support activities, such as mutual aid agreements, standard operating procedures, and policy development. Personnel should be trained on the latest security, resiliency, continuity and operational practices and maintain in-service training as new technology and methods are made available.

Despite every effort, cyber threat events will occur. Being prepared to execute response processes and procedures, prevent expansion of the event, mitigate its effects, and eradicate the incident is necessary. Incident response plans, recovery or resiliency plans, and continuity of operations plans are useful in cybersecurity incident response. Recovery planning processes and strategies are improved by incorporating lessons learned into future activities.

Cybersecurity Framework

The National Institute of Standards and Technology (NIST) developed the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) as a flexible and voluntary risk-based approach that outlines techniques to secure critical infrastructure. Recipients are strongly encouraged to implement NIST's framework to complement an existing risk management process or to develop a credible program if one does not exist. The Critical Infrastructure Cyber Community C³ Voluntary Program supports owners and operators of critical infrastructure, academia, Federal Government, state, local, tribal, and territorial governments, and businesses in their use of the Cybersecurity Framework.

The NIST Cybersecurity Framework establishes five functions to integrate cybersecurity into mission functions and operations, including: 1) ***identify***, evaluate, and prioritize risks for their entity; 2) ***protect*** against identified risks; 3) ***detect*** risks to the network as they arise; 4) deploy ***response*** capabilities to mitigate risks; and 5) establish ***recovery*** protocols to ensure the resiliency and continuity of communications. DHS's Emergency Services Sector has developed tailored guidance specific to emergency service disciplines, including a NIST Framework implementation guide with a repeatable process to identify and prioritize cybersecurity improvements.[1]

[1] Suggested resources include the *2015 ESS Cybersecurity Framework Implementation Guidance* and *2014 ESS Roadmap to Secure Voice and Data Systems*.

There is considerable cybersecurity guidance available from government, industry, and academic organizations and a multitude of standards development organizations (SDOs) that contribute to technical standards and best practices. Organizations managing critical infrastructure will continue to have unique risks—different threats, different vulnerabilities, and different risk tolerances—and how they implement the standards and guidance available will vary. There is currently no one-size-fits-all network cybersecurity solution. Table B-2 lists the applicable standards for cybersecurity that recipients should leverage as they identify and select the standards that fit their system and mission needs. Table B-3 lists cybersecurity resources for additional information. While these lists are not exhaustive, they include some of the more comprehensive guidance for the public safety community.

Table B-2. Cybersecurity Standards

Organizations	Standards
Third Generation Partnership Project (3GPP) Security Standards	3GPP's security working group, SA3, is continuously updating security standards associated with prevalent technologies, most notably IP Multimedia Subsystem. Specifically, the group is addressing 3GPP standards for network access security, network domain security, user domain security, application domain security, and user configuration and visibility of security is important for critical infrastructure implementations. www.3gpp.org.
American National Standards Institute (ANSI) / International Society of Automation (ISA)	ANSI/ISA standards focus on automation and control systems solutions. The NIST Cybersecurity Framework recommends two ANSI/ISA standards for use: ANSI/ISA-62443-2-1 (99.02.01)-2009 and ANSI/ISA-62443-3-3 (99.03.03)-2013. https://www.isa.org/templates/two-column.aspx?pageid=131422. Also, outputs of the Alliance for Telecommunications Industry Solutions (ATIS) Emergency Services Interconnection Forum, Next Generation Interconnection Interoperability Forum, and Wireless Technologies and Systems Committee are important to the public safety community.
Criminal Justice Information Services (CJIS) Security Policy	CJIS standards contain information security requirements, guidelines, and agreements reflecting the will of law enforcement agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information. https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.
European Telecommunications Standards Institute (ETSI)	ETSI Telecommunications & Internet converged Services & Protocols for Advanced Networks (TISPAN) has been a key standardization body in creating Next Generation Network (NGN) specifications, and their Cyber Security committee focuses entirely on privacy and security activities. Of note for emergency communications are the ETSI TS 102, 123, 182, and 282 series. http://www.etsi.org/.
Federal Information Processing Standards (FIPS)	FIPS establishes the minimum security requirements for federal information systems. https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Legislation enacted by Congress in 1997 to streamline medical regulations, privacy considerations, and the efficiency and security of medical care. The standards/rules associated with HIPAA address some of the NIST Cybersecurity Framework functions. https://www.hhs.gov/hipaa/.
International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Standards	The ISO/IEC 27000 series of standards provide a foundation for information security management best practices. Of interest to emergency communication networks may be ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27002, ISO/IEC 27032, and ISO/IEC 17799. http://www.iso.org.
Institute of Electrical and Electronics Engineers (IEEE)	IEEE produces sector-specific security standards, as well as industry guidance. Of interest to networks may be the 802, 1363, and 1619 series, as well as C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. http://www.ieee.org/.
International Telecommunication Union (ITU)	A fundamental role of ITU is to build confidence and security in the use of Information and Communication Technologies. Of note for emergency communications networks include X.800, X.805, and X.1051. http://www.itu.int/.

Organizations	Standards
Internet Engineering Task Force (IETF)	IETF Working Groups are the primary mechanism for development of IETF standards. IETF Working Groups currently have 598 standards regarding security mechanisms, integrity mechanisms, network layer security, transport layer security, application layer security, encryption algorithms, key management, secure messaging, etc. https://www.ietf.org/.
National Fire Protection Association 1221	A standard for the installation, maintenance, and use of emergency services communications systems, including cybersecurity considerations. http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1221.
NIST Recommendations on Cybersecurity (Special Publications 800 Series)	NIST's 800 series provides targeted cybersecurity guidance and are strongly encouraged to be incorporated into cybersecurity planning. http://csrc.nist.gov/publications/PubsSPs.html.
North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Regulations	Reliability standards address the security of cyber assets essential to the reliable operation of the electric grid. With emerging interconnectivity of infrastructure, the emergency communications community may also need to address these standards. http://www.nerc.com/pa/CI/Comp/Pages/default.aspx.
Telecommunications Industry Association (TIA)	TIA has both Cybersecurity and Public Safety working groups. Standards of particular use for emergency communications include: TR-8, TR-30, TR-34, TR-41 TR-42 TR-45, TR-47, TR-48, TR-49, TR-50 M2M, TR-51, and TIA-102. https://www.tiaonline.org/.
World Wide Web Consortium (W3C)	Includes web cryptography, web application security, web payments, and XML security. https://www.w3.org/.

Table B-3. Cybersecurity Resources

Organizations	Resources
Committee on National Security Systems (CNSS)	• CNSS Policies
Department of Homeland Security	• C^3 Voluntary Program Cyber Resilience Review • Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan • Continuous Diagnostics and Mitigation (CDM) • Cybersecurity Evaluation Tool (CSET) • Emergency Services Sector (ESS) Cyber Risk Assessment – 2012 • ESS Roadmap to Secure Voice and Data Systems – 2014 • ESS Cybersecurity Framework Implementation Guidance – 2015 • Emergency Services Sector-Specific Tabletop Exercise Program (ES SSTEP) • Homeland Security Grant Program Supplemental Resource: Cyber Security Guidance • Intrusion Detection (IDS) and Intrusion Prevention (IPS) • Information Sharing Environment (ISE) Guides and Best Practices • National Cyber Incident Response Plan • National Cybersecurity and Communications Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT) • National Infrastructure Coordinating Center (NICC) • National Infrastructure Protection Plan • Network Flow Collection • Safeguarding and Securing Cyberspace • Supplement Tool: Executing a Critical Infrastructure Risk Management Approach • Supplement Tool: National Protection and Programs Directorate Resources to Support Vulnerability Assessments • Trusted Internet Connections • Guidelines for Encryption in Land Mobile Radio Systems • Best Practices for Encryption in Project 25 Public Safety Land Mobile Radio Systems

Organizations	Resources
Department of Energy	• Energy Sector Cybersecurity Capability Maturity Model (C2M2) Program
Executive Orders (EO) and President Directives	• EO 13636: Improving Critical Infrastructure Cybersecurity • EO 13231: Critical Infrastructure Protection in the Information Age and EO 13286 • EO 13618: Assignment of national Security and Emergency Preparedness Communications Functions • Executive Office of the President, Presidential Policy Directive 21 (PPD – 21) • EO 13407: Public Alert and Warning System
Federal Bureau of Investigation	• Internet Crime Complaint Center
Federal Communications Commission	• Communications Security, Reliability and Interoperability Council (CSRIC) • Task Force on Optimal PSAP Architecture (TFOPA) • Cyber Security Planning Guide
Federal Emergency Management Agency	• Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC)
Government Accountability Office	• U.S. Government Accountability Office, Cybersecurity
National Institute of Standards and Technology	• Framework for Improving Critical Infrastructure Cybersecurity • Internal/Interagency Reports (NISTIRs) • National Initiative for Cybersecurity Education (NICE) • NICE Cybersecurity Workforce Framework
Various Industry and Associations	• ATIS Industry Best Practices • Association of Public-Safety Officials, International (APCO), specifically SPCO Cybersecurity Guide for Public Safety Community Professionals and APCO Introductory Guide to Cybersecurity for PSAPs ISACA COBIT 5 Framework • ITU Security Standards Roadmap • SANS Institute 20 Critical Security Controls • National Association of State Chief Information Officers (NASCIO) Cybersecurity Awareness, including NASCIO Cyber Disruption Planning Guide for States • National Conference of State Legislation Cybersecurity Training for State Employees • Open Web Application Security Project (OWASP) Top Ten Project • OWASP Internet of Things Project

Land Mobile Radio	
	Grant recipients should purchase digital LMR systems and equipment compliant with the P25 suite of standards, and include all applicable P25 standards and expectations for interoperability in any SOW or acquisition documents
	Recipients should purchase P25 compliant systems and equipment that has been assessed as compliant in accordance with the P25 Compliance Assessment Program
	If encryption is required, agencies shall ensure compliance with the P25 Block Encryption Protocol standard and implement Advanced Encryption Standard 256-bit encryption
	Recipients should ensure all P25 eligible equipment, features, and capabilities selected are P25 compliant, to include new equipment and upgrades
	When purchasing bridging or gateway devices that have a VoIP capability to provide connectivity between LMR systems, those devices should, at a minimum, implement either the BSI specification or the ISSI

LMR systems are terrestrially-based, wireless, narrowband communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works companies, and the military in non-tactical environments, to support voice and low-speed data communications. These systems are designed to meet public safety's unique mission and critical voice requirements and support time-sensitive, lifesaving tasks, including sub-second voice call-setup, group calling capabilities, high-quality audio, and priority access to the end-user. Because LMR systems implemented by the public safety community support lifesaving operations, they are designed to achieve high levels of reliability, redundancy, coverage, and capacity, and can operate in harsh natural and man-made environments. LMR technology has progressed over time from conventional, analog voice service to complex systems incorporating digital and trunking features. These enhancements have improved the interoperability, spectral efficiency, security, reliability, and functionality of voice and low speed data communications.

For the foreseeable future, the public safety community is expected to follow a multi-path approach to develop, establish, and maintain critical communications capabilities. To improve interoperability across investments, grant recipients are strongly encouraged to ensure digital voice systems and equipment purchased with federal grant funds are compliant with the Project 25 (P25) suite of standards, unless otherwise noted in a program's grant guidance.[2] Recipients should ensure all P25 eligible equipment, features, and capabilities selected are P25 compliant, to include new equipment and upgrades. When federal grant funds are used to purchase P25 LMR equipment and systems that contain non-standard features or capabilities, while a comparable P25 feature or capability is available, recipients must ensure the standards-based feature or capability is included.

Grant recipients should purchase P25 compliant systems and equipment that has been assessed as compliant in accordance with the P25 Compliance Assessment Program (P25 CAP). P25 standards

[2] Applicants should read grant guidance carefully to ensure compliance with standards, allowable cost, documentation, reporting, and audit requirements. If interested in using federal funds to purchase equipment that does not align with P25 standards or does not appear on the approved equipment list, the applicant should consult with the federal grant-making agency to determine if non-P25 compliant equipment is allowable. In some cases, written justification must be provided to the grantor. Many agencies will not approve non-standards-based equipment unless there are compelling reasons for using other solutions. Authorizing language for most emergency communications grants strongly encourages investment in standards-based equipment. Funding requests by agencies to replace or add radio equipment to an existing non-P25 system (e.g., procuring new portable radios for an existing analog system) will be considered if there is a clear rationale why such equipment should be purchased and written justification of how the equipment will advance interoperability and support eventual migration to interoperable systems. Written justification should also explain how that purchase will serve the needs of the applicant better than equipment or systems that meet or exceed such standards. Absent compelling reasons for using other solutions, agencies should invest in standards-based equipment.

provide many technical specifications for that are designed to ensure equipment is interoperable regardless of manufacturer. Recipients should obtain documented evidence of P25 compliance from the manufacturer that the equipment has been tested and passed all the applicable, published, normative P25 compliance assessment test procedures for performance, conformance, and interoperability as defined in the latest P25 Compliance Assessment Bulletins for testing requirements. If documentation for applicable equipment is not available through the P25 CAP or there is an absence of applicable testing in the P25 CAP, recipients should obtain documented evidence from the manufacturer stating that the applicable tests were conducted in accordance with the published test procedures in the P25 suite of standards.

Grant recipients using federal funds to purchase encryption options for new or existing communications equipment shall ensure encrypted capabilities are compliant with the published P25 Block Encryption Protocol Standard. Recipients investing in encryption must implement the Advanced Encryption Standard (AES) 256-bit Encryption Algorithm as specified in the P25 Block Encryption Protocol. The P25 suite of standards references the use of AES as the primary encryption algorithm but continues to allow Data Encryption Standard-Output Feedback (DES-OFB) for backwards compatibility and interoperability with existing systems. The current version of the P25 Block Encryption Protocol, ANSI/TIA-102.AAAD should be identified in all procurement actions when encryption is required.

Recipients seeking to use federal grant funds to purchase non-standard encryption features (e.g., 40-bit encryption, DES-OFB) or capabilities for new or existing equipment must ensure AES 256-bit is also included to ensure their devices have the capability to interoperate in an encrypted mode. Agencies currently using DES-OFB may continue to invest in this encryption method but should plan to migrate to AES as soon as possible. The continued use of DES-OFB or other non-standard encryption algorithms is strongly discouraged. The Federal Government recognizes AES as a more robust encryption algorithm and strongly recommends entities migrate to AES as it will enhance interoperability with federal entities, as well as state and local agencies implementing encryption in the future.

When purchasing bridging or gateway devices that have a VoIP capability to provide connectivity between LMR systems, those devices should, at a minimum, implement either the Bridging System Interface (BSI) specification or the P25 Inter Radio Frequency Sub-System Interface (ISSI) as a part of their VoIP capability.

The P25 Steering Committee periodically published a list of *Approved Project 25 Suite of Standards* that includes the most recent documents and revisions. Also, the *P25 Technology Interest Group's Capabilities Guide* can help determine which standards are applicable to proposed purchases and projects.

Table B-4. Land Mobile Radio Standards and Resources

Organizations	Standards and Resources
P25 Compliance Assessment Program	P25 CAP is a partnership of the DHS Office for Interoperability and Compatibility, industry, and the emergency response community. It is a formal, independent process for ensuring communications equipment declared by the supplier is P25 compliant and tested against the standards with publicly published results. The P25 CAP publishes Compliance Assessment Bulletins on policy, testing, and reporting requirements, as well as an approved equipment list that may be eligible for grant funds.
Telecommunications Industry Association	TIA is a recognized American National Standards Institution SDO responsible for publishing the P25 suite of standards. To date, TIA has published over 90 documents detailing the specifications, messages, procedures, and tests applicable to the 11 interfaces, multiple feature sets, and functions offered by P25. Test documents include performance, conformance, and interoperability procedures to ensure baseline compliance with the applicable published and accredited technical standards.

Public Safety Broadband	Applicants interested in investing federal funds in broadband-related infrastructure projects should consult the federal granting agency to understand all requirements and restrictions impacting broadband investments Grant recipients should consult with any applicable governing bodies and FirstNet to ensure the project does not conflict with network deployment efforts Recipients may be able to use grant funds for the implementation of alternative broadband technologies and the deployment of fiber optic backhaul networks in rural and unserved areas

Applicants investing in broadband technologies should be aware that the Federal Government is developing a Nationwide Public Safety Broadband Network (NPSBN). The First Responder Network Authority's (FirstNet) mission is to deploy, operate, and maintain the NPSBN to provide long-term evolution (LTE)-based broadband services and applications to public safety entities. The network is a single, nationwide network architecture consisting of a core network, transport backhaul, and radio access network (RAN). The development of technical standards for the network is underway, and statewide planning to identify users and assess needs is in progress.

Applicants are encouraged to engage in planning for the NPSBN at the state-level. Applicants proposing the acquisition and deployment of broadband projects that will operate in the 700 megahertz (MHz) public safety broadband spectrum (758–769 MHz and 788–799 MHz) should be aware that federal granting agency will review broadband-related proposals closely. Applicants should demonstrate in applications that the project:

- Has authority from FirstNet to operate in the public safety broadband spectrum;
- Has been coordinated with statewide broadband planners;
- Supports the statewide plan for broadband;
- Complies with FirstNet technical requirements; and
- Will integrate into the NPSBN.

Applicants should coordinate with FirstNet in advance of any strategic acquisition of LTE equipment to ensure understanding of all requirements and restrictions impacting broadband investments and that purchases support future service choices. Applicants should also monitor federal actions affecting broadband investments and continue planning and outreach activities (e.g., community education, documenting user needs) and to work with applicable governing bodies in planning for the arrival of broadband and other advanced technologies, including:

- Planning for integration of Information Technology infrastructure, software, and site upgrades necessary to connect to FirstNet;
- Broadband devices including smartphones, feature phones, tablets, wearables, laptops, ruggedized smartphones, ruggedized tablets, USB modems/dongles, in-vehicle routers, and Internet of Things devices;
- Customer-owned and managed broadband deployable equipment, enabling public safety to own and dispatch coverage expansion or capacity enhancement equipment within their jurisdiction;
- Broadband device accessories that enable efficient and safe public safety operations such as headsets, belt clips, ear pieces, remote Bluetooth sensors, and ruggedized cases;
- FirstNet SIM/UICC card to allow public safety users to update existing devices, "Bring Your Own Device", and new devices to operate on public safety prioritized services; and
- One-time purchase and subscription-based applications for public safety use which could include, among several other options, enterprise mobility management, mobile Virtual Private Network, identity services, or cloud service tools.

Non-LTE wireless broadband technologies, such as Wi-Fi, WiMAX, and mesh networks, are sometimes used to supplement public safety communications. These solutions, which are either agency-owned or provided by a commercial provider, allow agencies to access voice, data, and video applications. Grant recipients should consider the overall impact of using other wireless broadband technologies given ongoing advancements in FirstNet's deployment and unique interoperability challenges introduced by each of the various technologies.

With these cautions, applicants may be able to use federal grant funds for costs related to the implementation of alternative broadband technologies and the deployment of fiber optic backhaul networks in rural and unserved areas. Applicants should work closely with federal granting agency and commercial suppliers and providers to ensure grant-funded systems and equipment will be compatible and interoperable with current and future solutions. Applicants are encouraged to implement innovative solutions that will yield improvements to communications capabilities and help the agencies plan for and prepare for the deployment of the NPSBN.

Table B-5. Broadband Technology Standards and Resources

Organizations	Standards and Resources
FirstNet	The Middle Class Tax Relief and Job Creation Act of 2012 created FirstNet as an independent authority within the National Telecommunications and Information Administration to provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety: https://www.firstnet.gov.
3GPP	3GPP is the SDO responsible for development and maintenance of LTE specifications, though various standards from TIA, ATIS, the Groupe Speciale Mobile Association (GSMA), and the Open Mobil Alliance (OMA) also contribute to LTE functionality and interoperability.
IEEE	The 802.11a, 802.11b/g/n, and 802.11ac wireless standards are collectively known as Wi-Fi technologies and developed and maintained by IEEE. The Official IEEE 802.11 Working Group Project Timelines provides status of each networking standard under development, and a link to each effort. IEEE also maintains the WiMAX family of 802.16 standards.

Alerts, Warnings, and Notifications	Grant recipients using funds to cover costs associated with AWN systems should: • Establish strong governance and engage in collaboration with existing AWN stakeholders • Ensure well-documented and field-tested plans, policies, and procedures, are executed, evaluated for potential gaps, and adapted to evolving AWN capabilities • Invest in secure and resilient AWN solutions, and incorporate safeguards to ensure the accuracy of messaging • Consider diversity and inclusion influence accessibility to AWN issuances, as well as how people receive, interpret, and respond to messages • Invest in solutions that enable comprehensive, targeted, specific, and transparent messaging, while minimizing issuance and dissemination delays • Select software or equipment that also supports regional operable and interoperable solutions If accessing IPAWS, grant recipients should select equipment and applications that adhere to both Common Alerting Protocol and IPAWS Profile standards

During an emergency, alerts, warnings, and notifications (AWNs) enable public safety officials to provide the public with information quickly. The Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS) is an Internet-based capability that federal, state, local, tribal, and territorial authorities can use to issue critical public alerts and warnings. IPAWS is accessed through software that meets IPAWS system requirements. There is no cost to send messages through IPAWS, although there may be costs associated with acquiring compatible alert origination software. IPAWS is not mandatory and does not replace existing methods of alerting, but instead complements existing systems and offers new capabilities.

FEMA built IPAWS to ensure that under all conditions the President of the United States can alert and warn the American people. Federal, state, local, tribal, and territorial authorities also have the opportunity to use IPAWS to send alerts and warnings within their jurisdictions. IPAWS improves alert and warning capabilities by allowing authorities to deliver alerts simultaneously through multiple communications devices reaching as many people as possible to save lives and protect property. These communication pathways include:

- Emergency Alert System (EAS) used by authorities to send detailed warnings via broadcast, cable, satellite, and wireline radio and television channels;
- Wireless Emergency Alerts (WEA) sent to mobile devices like a text message, even when cellular networks are overloaded and can no longer support person-to-person calls, texts, or emails;
- National Weather Service Dissemination Systems, including the National Oceanic and Atmospheric Administration (NOAA) Weather Radio;
- Unique Alert Systems that have permission to retrieve alerts directly from IPAWS and deliver the alerts to their customer base; and
- Future Systems, including computer gaming systems, digital signs, siren systems, Internet search engines, social sharing websites, instant messaging, and others that are or could use IPAWS.

In order to access IPAWS, grant recipients should select equipment and applications that adhere to both the Common Alerting Protocol (CAP) and IPAWS Profile standards. Alert and warning software and equipment is developed, produced, and distributed by various vendors. While the Federal Government does not endorse any specific vendor, piece of software, or equipment, grant recipients should confirm vendors meet CAP and IPAWS Profile standards, provide support services, and include basic security measures (e.g., firewalls, anti-virus tools, anti-spyware tools) and strong access controls requiring authentication of users. A key consideration is access to the service through jammed or damaged communications channels during a real emergency. Recipients should also consider factors affecting continuity of operations, such as support of remote employees, mobile alerting capabilities, and contingent operations in disruptive circumstances.

To maintain AWN issuance proficiencies, agencies sending alerts should conduct trainings, exercises, and tests of systems on a regular basis. Lessons observed from these activities and incidents should be evaluated, documented, and incorporated into future operations. Alert originators should also work to minimize issuance delays, from the point of a hazard's detection to dissemination, by creating message templates, expediting information sharing, identifying and establishing triggers, and avoiding ad-hoc decision making.

Agencies are encouraged to coordinate with regional partners and submit applications that promote regional (e.g., multi-jurisdictional, cross-state, cross-border) collaboration and cost-effective measures. AWN grant funds should focus on eligible public alert and warning activities to include, but not limited to the purchase, training, exercising, replacement, and maintenance (e.g., annual license, subscription fees, upgrades) of alert and warning systems, software, and equipment.

Table B-6. AWN Standards and Resources

Organizations	Standards and Resources
Common Alerting Protocol (CAP)	The CAP standard is an open, non-proprietary digital format for exchanging emergency alerts that was developed by Organization for the Advancement of Structured Information Standards (OASIS). CAP allows a consistent alert message to be disseminated simultaneously over many different dissemination mechanisms. The CAP format is compatible with emerging technologies, such as web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' NOAA Weather Radio and the EAS, while offering enhanced capabilities including images, maps, and video.
OASIS	FEMA worked with OASIS to develop a standardized international technical data profile that defines a specific way of using the standard for the purposes of IPAWS. The CAP standard and supplemental IPAWS Profile ensure compatibility with existing warning systems. Latest CAP: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#tc-tools.
FEMA Integrated Public Alert and Warning System (IPAWS)	The IPAWS Program Management Office (PMO) does not endorse any specific vendor, piece of software, or equipment. Test results for any alert and warning software or equipment tested at the IPAWS Lab can be made available to assist agencies in making procurement decisions by contacting the IPAWS PMO at ipaws@dhs.fema.gov.

911 Systems	Grant recipients using funds to cover costs associated with 911, Enhanced 911 (E911), or Next Generation 911 (NG911) should rely on current guidance from the National 911 Program

The National 911 Program, administrated by the Department of Transportation National Highway Traffic Safety Administration, provides federal leadership and coordination in supporting and promoting optimal 911 services. This federal home for 911 plays a critical role by coordinating federal efforts that support 911 services across the Nation.

NG911 will seamlessly connect public safety answering points (PSAPs) and allow for the transmission and reception of multimedia type data (e.g., text messages, pictures, and video). As NG911 standards continue to evolve, applicants should consult the *NG911 Standards Identification and Review* to ensure that solutions developed or procured meet industry guidelines and standards. Applicants should consider the following when planning and implementing NG911:

- Strive for IP-enabled NG911 open standards and understand future technology trends to encourage system interoperability and emergency data sharing
- Establish collaborative relationships and policy mechanisms that facilitate the ongoing coordination required to plan, deploy, operate, and maintain NG911 systems
- Determine the responsible entity(ies) and mechanisms for geospatial data acquisition, reconciliation, and synchronization that are required for NG911
- Establish system access, security controls, and comprehensive cybersecurity plans to protect and manage access to NG911
- Ensure formalized governance models are in place to aid in the transition from legacy 911 to NG911
- Develop and implement sustainable funding models that support the planning, design, deployment, and ongoing operation of NG911
- Develop contract language that ensures the accountability of contractors in building, testing, deploying, operating, and maintaining interoperable and secure NG911 systems

Table B-7. NG911 Standards and Resources

Organizations	Standards and Resources
National 911 Program Office	The National 911 Program also provides the 911 community with a collection of documents, website links and other resources generated by both the program and other industry experts. These vetted resources address topics including emerging emergency communications technologies, wireless deployment, E911 location accuracy, cybersecurity, FirstNet, NG911, governance and 911 legislation, and are located in the Document and Tools section of the National 911 Program's website.
911 Grant Program	The Middle Class Tax Relief and Job Creation Act of 2012 authorized $115 million for a targeted 911 Grant Program administered by the Departments of Transportation and Commerce. Visit https://www.911.gov/project_911grantprogram.html for information and sign up for webinars and newsletters. Other federal programs fund 911; for a list of federal grant and loan programs that may allow 911 activities, visit: https://www.911.gov/federal_grants_opportunities.html.
National Emergency Number Association (NENA) Security for NG911 Standard	Standards of note for NG911 networks include NENA-STA-010: Detailed Functional and Interface Specification for the NENA i3 Solution; NENA 75-001: NENA Security for NG911 Standard (NG-SEC); NENA 75-502: NG-SEC Audit Checklist; NENA 04-503: Network/System Access Security Information Document, and NENA-INF-015.1-2016: NG911 Security Information Document. http://www.nena.org/.
NG911 Standards Identification and Review	Collection of resources from all major standards bodies that address cybersecurity when planning for NG911 deployments: https://www.911.gov/documents_tools.html.

Data Exchange and Information Sharing Environments	Agencies should perform an evaluation of who the organization most often communicates with, and what types of information are commonly exchanged Grant recipients using federal funds for data exchange solutions should ensure the solutions comply with OASIS EDXL suite of data messaging standards and NIEM framework For any grant funding software-based patient tracking products, the product is strongly encouraged to comply with OASIS EDXL-TEP, Bi-directional Transformation of OASIS EDXL-TEP (Tracking of Emergency Patients) v1.1, and HL7 v2.7.1 Specification Version

Data exchange and information sharing solutions are as fundamental as a digital data "snapshot" transferred over electronic media, or as tailored as custom-interface applications that allow proprietary applications to be linked. Challenges for effective information exchange include increasing types of data being exchanged, such as geographic information systems, evacuee or patient tracking, biometrics, accident and crash telematics, Computer-Aided Dispatch, Automatic Vehicle Location, and more. To communicate seamlessly with the increasingly interconnected systems of the broader community, agencies should consider standards-based information exchange models. A few of widely used exchange models are provided as part of this appendix; however, an evaluation of who the organization most often communicates with, and what types of information are commonly exchanged, is recommended in selecting an ideal data exchange and information sharing solution.

The National Information Exchange Model (NIEM) is a framework for exchanging information that provides common terminology for users and a repeatable, reusable process for developing information exchange requirements. NIEM was established by the Departments of Justice and Homeland Security in 2005 to unite stakeholders from federal, state, local, and tribal governments and the private sector, to develop and deploy a national model for information sharing and the organizational structure to govern it. Today, all 50 states and many federal agencies are using or considering NIEM, including adoption by the Departments of Agriculture, Defense, Health and Human Services, and Transportation. NIEM allows disparate systems to share, exchange, accept, and translate information in an efficient manner that all users can understand.

In addition to the NIEM framework, agencies should reference the Global Reference Architecture (GRA) and the OASIS Emergency Data eXchange Language (EDXL) suite of data messaging standards. Applicable standards include the CAP; distribution element; hospital availability exchange; resources messaging; reference information model; situation reporting; and tracking emergency patients.

- Global Reference Architecture provides guidance for agencies to develop and establish a service-oriented architecture for public safety information sharing. The GRA incorporates and reuses appropriate subsets of the NIEM, as well as other models such as the Global Federated Identity and Privilege Management (GFIPM) sponsored by the Departments of Justice and Homeland Security. The GRA provides practitioners with overarching guidance that demonstrates how federal initiatives, including NIEM and GFIPM, work together and how to accelerate the planning process. Agencies can use this GRA tool to develop a well-conceived, formal approach to designing information sharing solutions and systems. A key benefit of a reference architecture is it helps promote consistent thinking and approaches among the people who use it, even if they have not shared information with each other.

- OASIS EDXL suite of data messaging standards facilitates information sharing among public safety agencies. Grant-funded systems, developmental activities, or services related to emergency response information sharing should comply with the following OASIS and HL-7 standards: "OASIS EDXL-TEP" and Bi-directional Transformation of OASIS EDXL-TEP (Tracking of

Emergency Patients) v1.1 and HL7 v2.7.1 Specification Version and OASIS EDXL suite of data messaging standards. Compliance should include the following OASIS EDXL standards:

- Common Alerting Protocol, version 1.2 or latest version
- Distribution Element (DE), version 1.0 or latest version
- Hospital AVailability Exchange (HAVE), version 1.0 or latest version
- Resource Messaging (RM) standards, version 1.0 or latest version

Table B-8. Data Exchange Standards and Resources

Organizations	Standards and Resources
NIEM	Applicants are encouraged to reference the NIEM website to develop a greater understanding of data exchange functions and processes.
GRA	Many Department of Justice grant solicitations require its grant recipients to comply with the GRA, specifically the Global Standards Package, which describes a full information sharing technology standards implementation suite that addresses data standardization, messaging architecture, security, and privacy requirements. For additional information, including technical assistance and training opportunities, visit the Office of Justice Programs website at: https://it.ojp.gov/initiatives/gra.
OASIS	OASIS Emergency Management Technical Committee (EM-TC) creates incident- and emergency-related standards for data interoperability: Common Alerting Protocol; Emergency Data Exchange Language Distribution Element (EDXL-DE); Emergency Data Exchange Language Resource Messaging (EDXL-RM); Emergency Data Exchange Language – Tracking of Emergency Clients (EDXL-TEC). https://www.oasis-open.org/.

Continuity and Resilience	Grant recipients should target funding toward activities that address communications continuity, survivability, and resiliency. Activities can include system assessments, analysis of threats and vulnerabilities, and strategic plan and procedural updates to mitigate identified risks.

Lessons learned from major disasters, unplanned events, and full-scale exercises have identified a need for greater coordination of emergency communications among senior elected officials, emergency management agencies, and first responders at all levels of government. Responders arriving on the scene of a domestic incident are not always able to communicate with other response agencies, particularly when the incident requires a multi-agency, regional response effort, or when primary communications capabilities fail. This lack of operability and interoperability between agencies is further complicated by problems with communications continuity, survivability, and resilience, which hinders the ability to share critical information, and can compromise the unity-of-effort required for an effective incident response.

Applicants investing in emergency communications are encouraged to work with Statewide Interoperability Coordinators, Statewide Interoperability Governance Bodies, and appropriate stakeholders across levels of government to:

- Establish robust, resilient, reliable, secure, and interoperable communication capabilities
- Plan for mission-related communications and connectivity among government leadership, internal elements, other supporting organizations, and the public under all conditions
- Trace all communications systems/networks from end-to-end to identify Single Points of Failure
- Recipients should also address the following issues:
    - Integrate communications needs into continuity planning efforts and emergency operations plans by incorporating mitigation options to ensure uninterrupted communications support
    - Maintain and protect communications capabilities against emerging threats, both man-made and natural, to ensure their readiness when needed
    - Frequently train and exercise personnel required to operate communications capabilities
    - Test and exercise communications capabilities
    - Establish a cybersecurity plan that includes continuity of an “out of band” communications capability such as High Frequency (HF) Radio Frequency (RF), fiber-based communications pathways that do not rely on public infrastructure
- Ensure key communications systems resiliency through:
    - Availability of backup systems
    - Diversity of network element components and routing
    - Geographic separation of primary and alternate transmission media
    - Availability of backup power sources
    - Access to systems that are not dependent on commercial infrastructure
    - Maintained spare parts for designated critical communication systems
    - Agreements with commercial suppliers to remediate communications Single Point of Failures

Table B-9. Continuity and Resilience Resources

Resource	Description
FEMA National Continuity Programs	National Continuity Programs highlight the national policy and guidance for continuity of operations initiatives. They provide guidance and assistance to support continuity preparedness for federal departments and agencies; state, local, tribal, and territorial government jurisdictions; and private sector organizations.
DHS Regional Resiliency Assessment Program	The Regional Resiliency Assessment Program is a cooperative assessment of specific critical infrastructure within a designated geographic area. DHS works with selected areas each year to conduct a regional analysis of surrounding infrastructure and address a range of resilience issues that could have significant regional or national consequences if disrupted.
DHS Ten Keys to Obtaining a Resilient Local Access Network	This document introduces resiliency concepts and provides ten keys to obtaining and maintaining resiliency in a local access network, such as knowing the exact network infrastructure in the local loop, interfacing with commercial service providers, and properly maintaining alternative path solutions. DHS developed these ten fundamental steps, supported by descriptive text and visually-appealing graphics, as recommendations to help organizations maintain critical communications in emergency situations.
DHS Priority Services Programs	Priority Services Programs, including the Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service, support national leadership; federal, state, local, tribal, and territorial governments; first responders; and other authorized national security and emergency preparedness users. They are intended to be used in an emergency or crisis situation when data, landline, or wireless networks are congested and the probability of completing a normal transmission or call is reduced.