Office of Emergency Communications:

Fiscal Year 2016

SAFECOM Guidance on Emergency Communications Grants

SAFECOM

U.S. Department of Homeland Security

A Message to Stakeholders

On behalf of the Office of Emergency Communications (OEC), I am pleased to present the *Fiscal Year 2016 SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance).* The *SAFECOM Guidance* is updated annually to provide current information on emergency communications policies, eligible costs, best practices, and technical standards for State, local, tribal, and territorial grantees investing Federal funds in emergency communications projects.

The *FY 2016 SAFECOM Guidance* aligns with the updated *National Emergency Communications Plan* (NECP). The 2014 NECP emphasizes the need to enhance the policies, governance structures, plans, and protocols that enable responders to communicate and share information under all circumstances. It aims to maximize the use of all communications capabilities available to public safety officials—voice, video, and data—and to ensure the security of data and information exchange. To accomplish this, grantees must engage the whole community in preparedness activities. Similarly, the *FY 2016 SAFECOM Guidance* addresses the rapidly evolving emergency communications ecosystem and encourages grantees to support the concepts and recommendations within the 2014 NECP.

This year's funding priorities remain consistent with previous *SAFECOM Guidance* releases. Grantees are strongly encouraged to coordinate with their statewide governance and emergency communications leaders (e.g., Statewide Interoperability Coordinators) to ensure projects support the State or territory's strategy to improve interoperable emergency communications. In addition, grantees should work with public and private entities, and across jurisdictions and disciplines, to assess needs, plan projects, coordinate resources, and improve response through cross-training and joint exercises.

The *SAFECOM Guidance* also encourages grantees to participate, support, and invest in planning activities that will help States or territories prepare for deployment of new emergency communications systems or technologies. At the same time, the *SAFECOM Guidance* recognizes the need to sustain current land mobile radio (LMR) systems. Grantees should continue developing plans and standard operating procedures, conducting training and exercises, and investing in standards-based equipment to sustain LMR capabilities, while concurrently planning for the deployment of new technologies. Grantees should also consider cybersecurity risks across all capabilities when planning operable, interoperable, and continuity of communications.

As in previous years, OEC developed the *FY 2016 SAFECOM Guidance* in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators. OEC also consulted Federal partners and the Emergency Communications Preparedness Center, to ensure that emergency communications policies are coordinated and consistent across the Federal Government. OEC encourages grantees to consult the *SAFECOM Guidance* when developing emergency communications investments, and to direct any questions to my office at oec@hq.dhs.gov.

Ron Hewitt, Director
Office of Emergency Communications
Department of Homeland Security

Contents

1. Introduction

The Department of Homeland Security (DHS) is mandated to administer responsibilities and authorities relating to the SAFECOM Program. Within DHS, the Office of Emergency Communications (OEC) is responsible for developing a coordinated guidance for Federal grant programs for public safety interoperable communications.[1] As a result, OEC develops the annual *SAFECOM Guidance on Emergency Communications Grants* (*SAFECOM Guidance*) for entities applying for Federal financial assistance for emergency communications projects. The *National Emergency Communications Plan* (NECP) defines emergency communications as the means and methods for exchanging communications and information for successful incident management.[2] The *SAFECOM Guidance* provides general information on eligible activities, technical standards, and other terms and conditions that are common to most Federal emergency communications grants.[3] The *SAFECOM Guidance* aims to ensure that emergency communications standards and policies across Federal grant programs provide a consistent approach to improving emergency communications nationwide.

SAFECOM is a public safety-driven communications program and OEC develops policy, guidance, and future efforts by drawing on SAFECOM member expertise and recommendations. The Office for Interoperability and Compatibility (OIC) within DHS' Science and Technology Directorate supports SAFECOM-related research, development, testing, evaluation, as well as the acceleration of standards. SAFECOM works to build partnerships among all levels of government, linking the strategic planning and implementation needs of the emergency response community with Federal, State, local, tribal, and territorial governments, to improve emergency communications. Additionally, OEC consulted members of the Emergency Communications Preparedness Center (ECPC) Grants Focus Group to better coordinate and develop a common guidance for Federal grant programs that support emergency communications.[4] Together, SAFECOM members and Federal partners coordinate on emergency communications policy and standards to ensure projects are compatible, interoperable, and most importantly, meet the needs of end-users.

1.1 Purpose of the FY 2016 SAFECOM Guidance

The *FY 2016 SAFECOM Guidance* provides guidance to grantees on:

- Recommendations for planning, coordinating, and implementing emergency communications projects
- Emergency communications activities that can be funded through Federal grants
- Overview of emergency communications systems and capabilities
- Technical standards that facilitate operability and interoperability

The *SAFECOM Guidance* is designed to promote and align with the national emergency communications goals established in the NECP. The updated NECP goals are strategic and aim

[1] 6 U.S.C. § 571(c)(2) and 6 U.S.C. § 574

[2] For more information on the NECP, see: http://www.dhs.gov/necp.

[3] Federal financial assistance includes grants, loans, cooperative agreements, and other financial assistance provided by the Federal Government. For the purposes of this document, these terms are used interchangeably, unless otherwise indicated.

[4] The Emergency Communications Preparedness Center (ECPC) Grants Focus Group is comprised of Federal grants officers, program administrators, and communications experts representing the 14 Federal agencies that participate in the ECPC.

to enhance emergency communications capabilities at all levels of government in coordination with the private sector, nongovernmental organizations, and communities across the Nation. The NECP's top priorities for the next three to five years address the people, processes, and technologies to enhance emergency communications. The 2014 NECP priorities are:

- Identifying and prioritizing areas for improvement in current land mobile radio (LMR) communications systems used by responders
- Ensuring emergency responders and government officials plan and prepare for the adoption, integration, and use of broadband technologies, including the development and deployment of the nationwide public safety broadband network (NPSBN)
- Enhancing coordination among stakeholders, processes, and planning activities across the broader emergency response community

The recommendations within the *SAFECOM Guidance* are intended to help State, local, tribal, and territorial stakeholders develop projects that meet critical emergency communications needs defined in the 2014 NECP and their Statewide Communication Interoperability Plan (SCIP).[5] Best practices and technical standards located within the *SAFECOM Guidance* help ensure that Federally-funded emergency communications investments are interoperable and support the national policies. However, not all of this guidance is applicable to all grant programs. Grants funding emergency communications are administered by numerous Federal agencies and are subject to various statutory and programmatic requirements. As a result, grantees should review specific grant guidance carefully to ensure their proposed activities are eligible, and that all standards, terms, and conditions required by the program are met.[6]

1.2 Report Methodology

OEC consulted with State and local stakeholders and Federal partners to develop the *FY 2016 SAFECOM Guidance* to include the priorities, recommendations, and technical standards. The priorities within this *SAFECOM Guidance* represent current needs and initiatives that stakeholders and Federal partners have recognized as integral to emergency communications and recommended to continue funding in FY 2016. Specifically, OEC consulted:

- Emergency Communications Preparedness Center
- Federal Communications Commission (FCC)
- National Council of Statewide Interoperability Coordinators (NCSWIC)
- National Institute of Standards and Technology (NIST)
- SAFECOM Executive Committee and SAFECOM[7]
- U.S. Department of Agriculture (USDA)
- U.S. Department of Commerce
    - First Responder Network Authority (FirstNet)
    - National Telecommunications and Information Administration (NTIA)
- U.S. Department of Homeland Security
    - Federal Emergency Management Agency (FEMA)

[5] For information on SCIPs, see the OEC website at: http://www.dhs.gov/statewide-communication-interoperability-plans.
[6] For the purposes of this document, "grant guidance" may include Funding Opportunity Announcements, Grant Notices, Grant Applications, and other formal notices of grants and Federal financial assistance programs.
[7] For a list of SAFECOM members, to include the National Public Safety Telecommunications Council, see SAFECOM's website at: http://www.dhs.gov/safecom/membership.

  - Integrated Public Alert and Warning System (IPAWS)
  - Office of the Chief Financial Officer
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Department of Transportation

1.3 Use of FY 2016 SAFECOM Guidance

The *FY 2016 SAFECOM Guidance* should be used during the planning, development, and implementation of emergency communications projects and in conjunction with other planning documents. Before proposing projects for funding, prospective applicants are encouraged to read the 2014 NECP, Federal and State preparedness documents such as statewide plans and reports, and the *FY 2016 SAFECOM Guidance* to ensure projects support Federal, State, local, tribal, and territorial plans for improving emergency communications. Table 1 provides a list of essential resources that are available to grantees.

Table 1. Essential Resources for Emergency Communications Grantees

Resources	Descriptions
NECP	The NECP is the only strategic national emergency communications plan that promotes communication and sharing of information across all levels of government, jurisdictions, disciplines, and organizations for all threats and hazards, as needed and when authorized. It provides information and guidance to those that plan for, coordinate, invest in, and use communications to support response operations. Grantees are encouraged to read the NECP to understand the national emergency communications strategy, and to ensure that investments support the goals and objectives of the Plan. The NECP is available at: http://www.dhs.gov/necp.
SCIP	The SCIP contains the State's strategy to improve emergency communications. Every State and territory was required to develop and submit a SCIP to OEC by December 2008, and is required to submit annually a report on the progress of the State in implementing its SCIP (i.e., SCIP Annual Snapshot). Many Federal grants funding emergency communications require grantees to align projects to needs identified in SCIPs and SCIP Annual Snapshots. Grantees should review the SCIP for their State and work with their SWIC to ensure that investments support, and do not contradict, statewide plans to improve communications. To find your State's SCIP, please contact your SWIC. To find the SWIC for your State or territory, contact OEC at: oec@hq.dhs.gov.
SAFECOM Website	The SAFECOM website provides information and resources for grantees developing emergency communications projects. For the most recent *SAFECOM Guidance* and list of grants funding emergency communications, see the SAFECOM website at: http://www.dhs.gov/safecom.
Office of Management and Budget (OMB) Grants Circulars	OMB provides grant resources on its Grants Management page at: http://www.whitehouse.gov/omb/grants_default/. Federal awards issued on or after December 26, 2014, must adhere to the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Grantees should reference specific Funding Opportunity Announcements to determine applicable requirements. Additional information is available on the Council of Financial Assistance Reform website at: https://cfo.gov/cofar/.

Resources	Descriptions
State Governance	The **Statewide Interoperability Governing Body (SIGB)** or **State Interoperability Executive Committee (SIEC)** serve as the primary steering group for the statewide interoperability strategy that seek to improve emergency response communications across the State through enhanced data and voice communications interoperability. SIGBs and SIECs include representatives from various jurisdictions, disciplines, as well as subject matter experts. To find the SIGB or SIEC for your State or territory, contact OEC at: oec@hq.dhs.gov.
	A **broadband working group** serves as the governing body for State or territory planning activities for the Nationwide Public Safety Broadband Network (NPSBN). Many States are using their SIGB or SIEC for planning or have created an independent working group focused on public safety broadband. Grantees are strongly encouraged to work with their respective group to ensure efforts do not contradict with FirstNet's planning with NPSBN.
	The **911 Advisory Board** works with the 911 Administrator to plan and coordinate State and local 911 efforts. The official title and role of this board vary by State or territory. Grantees are encouraged to coordinate 911 projects with the Board to ensure that projects support State or territory 911 efforts. To find your 911 Advisory Board, refer to the National 911 Profile Database at: http://www.nasna911.org/state-911-contacts.
State Leadership	The **Statewide Interoperability Coordinator (SWIC)** serves as the State single point of contact for interoperable communications and implements the SCIP in coordination with the SIGB or SIEC. Grantees are strongly encouraged to coordinate projects with the SWIC to ensure that projects support statewide efforts to improve emergency communications. To find the SWIC for your State or territory, visit http://www.dhs.gov/safecom or contact OEC at: oec@hq.dhs.gov.
	As required as a condition of the State and Local Implementation Grant Program (SLIGP), each State and Territory Governor designated an individual or body to serve as the **Single Point of Contact (SPOC)** to engage in consultation with FirstNet for the planning of the NPSBN and serve as coordinator for the SLIGP. Grantees are strongly encouraged to consult with the SPOC for their State or territory when engaging in public safety broadband activities. To find the FirstNet SPOC for your State or territory, refer to: http://firstnet.gov/consultation.
	The **State Emergency Management Agency Director** is responsible for ensuring that the State or territory is prepared to deal with any type of emergency, as well as coordinating statewide incident response. This includes collaborating with appropriate statewide representatives for critical capabilities, such as emergency communications. The Director may also have the responsibility for statewide 911 communications and public alerting.
	State Information Technology and Security Officials, including a State or territory's Chief Information Officer, Chief Technology Officer, and Chief Information Security Officer manage key information technology (IT) initiatives, including IT procurement, security, and IT planning and budgeting.
	The **911 Administrator** manages the State or territory's 911 functions as determined by State legislation. The official title and role of this position may vary by State or territory. Grantees are encouraged to coordinate 911 projects with the Administrator to ensure that projects support State or territory 911 efforts. To find your State or territory's 911 Administrator, refer to the National Association of State 911 Administrations at: http://www.nasna911.org/state-911-contacts.
	The **Homeland Security Director** coordinates the planning, development, and coordination of statewide policies developed in support of public and private organizations responsible for preventing terrorism, raising awareness, reducing vulnerabilities, responding to, and recovering from terrorist acts. To locate your State or territory's Homeland Security Director or office, refer to: http://www.dhs.gov/state-homeland-security-contacts.

1.4 Key Changes and Updates

This section highlights key changes to the *FY 2016 SAFECOM Guidance*:

- **Emergency Communications Priorities (Section 2).** This section reviews the FY 2016 priorities including: Governance and Leadership, Statewide Planning for Emergency Communications, Emergency Communications Training and Exercises, Activities that Enhance Operational Coordination, and Standards-based Technology and Equipment.

- **Before Applying (Section 3).** This section provides an updated overview of national policies, laws, and issues affecting emergency communications grants and the broader emergency communications ecosystem, as well as Federal requirements and restrictions on funding that grantees should consider before applying.

- **Eligible Activities (Section 4).** This section includes a review of eligible costs and has been updated to address 2014 NECP strategic goals and recommendations.

- **Emergency Communications Systems and Capabilities (Section 5).** This section provides an overview of emergency communications and the importance of deploying standards-based technology and equipment.

- **Grants Management Best Practices (Section 6).** This section provides best practices to ensure the effective implementation of grants and to establish the entity as a trusted steward of Federal grant funding and a credible recipient of future grant funding.

- **Funding Sources (Section 7).** This section offers recommendations on how grantees should consider multiple funding sources, including traditional grants and other sources that may partially fund emergency communications projects.

- **Appendices.** The Appendices include an acronym list, technical standards for emergency communications equipment, and resources grantees can reference when developing emergency communications projects. New for FY 2016, DHS has outlined specific requirements for DHS recipients. These requirements are in accordance with the DHS Standard Terms and Conditions of preparedness grants.

2. Emergency Communications Priorities

OEC is responsible for ensuring that grant guidelines and priorities relating to interoperable emergency communications are coordinated and consistent with the goals and recommendations in the NECP.[8] In support of this mandate, the *FY 2016 SAFECOM Guidance* identifies five investment priorities. These priorities were developed in coordination with stakeholders and Federal partners, and are informed by the 2014 NECP, as well as other applicable Presidential Policy Directives, Federal statutes, and regulations. In FY 2016, grantees are encouraged to target grant funding toward the following priorities:

- Priority 1: Governance and Leadership
- Priority 2: Statewide Planning for Emergency Communications
- Priority 3: Emergency Communications Training and Exercises
- Priority 4: Activities that Enhance Operational Coordination
- Priority 5: Standards-Based Technology and Equipment

2.1 Priority 1: Governance and Leadership

Strong governance and leadership structures are essential to effective decision-making, coordination, and planning for emergency communications. While the existence and growth in governance bodies is a significant accomplishment, many of these entities were originally established to address LMR interoperability issues. Evolving technology and rising expectations in emergency communications changes the traditional roles and responsibilities within the public safety community, requiring strong, broader scopes, and unified governing bodies. Fortunately, there is already a strong foundation for future progress. State, local, tribal, and territorial governments should focus on expanding or updating current structures, processes, and investments in governance and leadership.

In FY 2016, grantees are encouraged to invest in emergency communications governance and leadership structures for coordinating statewide and regional initiatives that reflect the evolving emergency communications environment.[9] These investments are critical for assessing needs, conducting statewide planning, coordinating investments, ensuring projects support the SCIP, maintaining and improving communications systems, and planning for future communications improvements. Governance and leadership structures can also facilitate the development of operating procedures and planning mechanisms that establish priorities, objectives, strategies, and tactics during response operations.[10]

To support this priority, grantees should target funding to:

- Sustain the SIGB or SIEC activities and SWIC position
- Update governance structures and processes to address the evolving operating environment, including:

[8] 6 U.S.C. §574

[9] See the *Governance Guide for State, Local, Tribal, and Territorial Emergency Communications Officials* at: http://www.dhs.gov/safecom/governance.

[10] See the *National Incident Management System* (NIMS) National Standard Curriculum Training Development Guidance at: http://www.fema.gov/national-incident-management-system.

- Include and coordinate with emergency communications leaders (e.g., FirstNet State Single POC, 911 leaders, Regional Emergency Communications Coordination Working Group [RECCWG], utilities commissions) and representatives from multiple agencies, jurisdictions, disciplines, levels of government, tribes, rural areas, subject matter experts, and private industry to share information on emergency communications and initiatives
- Review and update key operating documents for SIGB or SIEC (e.g., charters, agreements, policies, procedures) to ensure they are positioned to address new technology deployments and facilitate coordination with the SWIC
- Integrate emergency communications governance and leadership into broader statewide planning efforts (e.g., FirstNet State consultations, 911 system migration, IT enhancements) to ensure emergency communications needs are represented
- Increase regional structures or processes to foster multi-State coordination and information sharing
- Conduct outreach and education to continually assess and address user needs

2.2 Priority 2: Statewide Planning for Emergency Communications

The emergency communications community benefits from a comprehensive and inclusive approach to planning. States and territories engage multiple jurisdictions, disciplines, and levels of government in planning through the update of their SCIPs, incorporating all emergency communications needs. The SCIP serves as the primary strategic plan for emergency communications, while other plans outline specific operational coordination or tactical procedures. Updating plans and standard operating procedures (SOP) to address emergency communications gaps, new technologies, and stakeholder needs helps to improve emergency communications and response across the whole community. This continuous and comprehensive planning enables States to effectively identify, prioritize, and coordinate to ensure that proposed investments support statewide planning priorities.

In FY 2016, States and territories should continue to target funding toward planning activities, including updates of statewide plans, and ensure plans incorporate the capabilities and needs of all emergency communications systems. The goal of this priority is to ensure that emergency communications needs are continually assessed and integrated into State-level risk assessments and preparedness plans. Stakeholders are encouraged to target FY 2016 funding toward planning, stakeholder outreach, assessment of user needs, and other activities that will help to engage the whole community in emergency communications planning initiatives.

To support this priority, grantees should target funding toward critical planning activities, including the following:

- Update SCIPs and other plans and procedures to:
  - Reflect the 2014 NECP strategic goals and recommendations
  - Incorporate the whole community concepts[11]

[11] Per the *National Preparedness Goal*, whole community is formally defined as, "A focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of Federal, State, and local governmental partners in order to foster better coordination and working relationships."

  - Address findings and gaps identified in State-level preparedness reports, assessments, and After-Action Reports (AAR) from real-world incidents and planned exercises
  - Identify and address FCC directives affecting current or planned public safety communications systems (e.g., narrowband mandate, T-Band migration, systems operating in the 700 megahertz [MHz] public safety broadband spectrum, 800 MHz rebanding)
  - Incorporate a multifaceted approach to ensure the confidentiality, integrity, reliability, and availability of data
- Support statewide emergency communications and preparedness planning efforts through the allocation of funding to the following planning activities:
  - Conduct and attend planning meetings
  - Engage the whole community in emergency communications planning, response, and risk identification
  - Develop risk and vulnerability assessments (e.g., cyber, threat and hazard identification and risk assessment [THIRA])
  - Integrate emergency communications assets and needs into State-level plans
  - Coordinate with SWIC, State Administrative Agency (SAA),[12] and State-level planners (e.g., SPOC, 911 planners, utilities commissions) to ensure proposed investments align to statewide plans and comply with technical requirements

2.3 Priority 3: Emergency Communications Training and Exercises

NECP Goal Demonstrations, AARs, and similar assessments reveal that jurisdictions are better able to respond to emergencies due in part to regular training and exercises. Training and exercising help response personnel understand their communications roles and responsibilities during an emergency, as well as the processes for working with other agencies. Further, as communications technologies continue to evolve, the need for training and exercises becomes even greater to ensure personnel are proficient in using existing and new technologies.

In FY 2016, grantees should continue to invest in emergency communications-related training and exercises to address gaps identified in response and recovery operations. Grantees are encouraged to participate in training and exercises across all levels of government and with other entities that will better assist jurisdictions to prepare for disasters and identify, assess, and address capability gaps.

To support this priority, grantees should target funding toward certified training and exercise activities, including:

- Conduct *National Incident Management System* (NIMS)-compliant training (e.g., training in Incident Command System [ICS] and the ICS Communications Unit such as Communications Unit Leader [COML] and Communications Technician [COMT])[13]
- Improve States' and territories' ability to track and share trained Communications Unit personnel during response operations (e.g., include Communications Unit training plan within statewide plans such as the SCIP)

[12] Many Federal grants are awarded to a designated SAA who serves as the official grantee and administrator for the grant.
[13] Regular training on NIMS/ICS concepts is needed to ensure new and existing staff are proficient in NIMS/ICS concepts. For NIMS-compliant training, see: http://www.fema.gov/emergency/nims/NIMSTrainingCourses.shtm.

- Perform exercises that support and demonstrate the adoption, implementation, and use of the NIMS concepts and principles
- Hold cross-training and State, regional, or national level exercises to validate plans and procedures
- Provide training and exercises on new and existing systems, equipment, and SOPs
- Assess and update training curriculums and exercise criteria to reflect changes in the operating environment and plain language protocols
- Identify opportunities to integrate private and public sector communications stakeholders into training and exercises, as well as cost-effective approaches (e.g., distance learning)
- Offer cyber training and education on the proper use and security of devices and applications, phishing, malware, other potential threats, and how to guard against attacks

2.4 Priority 4: Activities that Enhance Operational Coordination

There has been significant improvement in capabilities at the State and local levels resulting in the ability of jurisdictions to more effectively coordinate communications resources and services during emergencies. This includes the integration of capabilities, resources, and personnel from across the whole community. As incidents escalate, communications resources must be able to expand rapidly to meet responders' needs. This requires States and territories to ensure they have an understanding of the communications resources to which they own or can access, as well as follow the appropriate procedures to request and deploy them to the locations where they are most needed.

In FY 2016, grantees are encouraged to update the inventories of their communications assets and share the information within their State or territory and with neighboring States that are most likely to request support during emergencies or events. This can be achieved by working with SWICs to update their inputs to the Next Generation Communication Assets Survey and Mapping (CASM NextGen) Tool—a web-based tool that assists public safety agencies to collect and visualize data, and assess inter-agency interoperability based on communications assets and interoperability methods.[14] Grantees should identify gaps in capabilities and target funding toward those gaps. In addition, grantees must continue to implement NIMS ICS principles during all emergencies. Grantees are also encouraged to actively engage neighboring jurisdictions—both internal and external to the State or territory—to coordinate response planning and seek mutual aid agreements for large-scale responses.

To support this priority, grantees should target funding to:

- Ensure inventories of emergency communications resources are updated and comprehensive
- Advance projects that promote assessment of communications assets, asset coordination, and resource sharing (e.g., CASM NextGen)
- Conduct risk and vulnerability assessments

[14] OEC developed a Public Safety Tools website, which provides support to the public safety community, including the CASM NextGen Tool, the Narrowband License Status Tool, the Response Level Communications Tool, and computer based training courses. For more information, see: http://www.dhs.gov/office-emergency-communications-technical-assistance-program.

- Develop, integrate, or implement SOPs, including Incident Action Plans and ICS Form 205 Incident Radio Communications Plans that enhance jurisdictions' ability to readily request communications resources or assets during operations
- Implement projects that promote regional, intra- and inter-State collaboration
- Inventory and typing of resources and other activities that strengthen resilience and provide backup communications solutions (e.g., radio caches)
- Address needs identified in statewide plans, AARs, or assessments
- Support communications initiatives that engage the whole community

2.5 Priority 5: Standards-based Technology and Equipment

In FY 2016, grantees should continue to invest in equipment that is standards-based to enable interoperability between agencies and jurisdictions, regardless of vendor. Grantees should include technical specifications in procurement agreements with vendors and obtain sufficient documentation to verify equipment is compliant to the applicable standards.

Grantees are strongly encouraged to invest in equipment that will help to sustain and maintain current LMR capabilities while planning for new technologies and capabilities that may not have fully defined standards. As emergency communications capabilities continue to evolve, grantees are strongly encouraged to participate in community outreach and planning to ensure new capabilities are interoperable and all user requirements are incorporated.

Grantees should improve their understanding of and preparations for the security risks associated with the use of Internet Protocol (IP)-based emergency communications systems. Cybersecurity is a key consideration for public safety officials as new technologies are integrated into their operations. This will require the public safety community to implement effective strategies to enhance the resiliency of cyber and IP-based infrastructures and safeguard private and sensitive information transmitted and stored by connected systems devices.[15]

To support this priority, grantees should target funding toward standards-based equipment that enables the entity to:

- Sustain and maintain current LMR capabilities
- Use Project 25 (P25)-compliant LMR equipment for mission critical voice communications[16]
- Support planning efforts for the deployment of the NPSBN while ensuring compliance with statewide plans and FirstNet requirements[17]
- Meet FCC and FirstNet spectrum and authority to operate requirements
- Transition towards Next Generation 911 (NG911) capabilities
- Support standards that allow for alerts and warnings across different systems
- Sustain backup solutions (e.g., backup power, portable repeaters, satellite phones, HF radios)
- Secure equipment, information, and capabilities from physical and virtual threats

[15] In February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity*, which is a voluntary risk-based approach to cybersecurity that uses industry guidelines to help organizations manage cyber risks to critical infrastructure. For more information, see: http://www.nist.gov/cyberframework.

[16] For more information on P25 requirements, see: http://www.project25.org/.

[17] Grantees interested in broadband investments should consult the SPOC for FirstNet requirements.

3. Before Applying

Before applying for Federal funds for emergency communications, grantees should:

- Review the NECP and SCIP
- Coordinate with statewide emergency communications leaders
- Recognize changes in the emergency communications ecosystem
- Understand Federal grant requirements and restrictions

3.1 Review the NECP and SCIP

Grantees should read the 2014 NECP to understand the national emergency communications strategy, and to ensure that proposed projects support national goals and objectives. Similarly, grantees should review their State or territory's SCIP to ensure that proposals support statewide plans to improve communications across all emergency communications systems and capabilities.

In addition to developing and updating SCIPs, OEC requests that each State and territory submit the SCIP Annual Snapshot (via SCIP@hq.dhs.gov) to document progress the State or territory has made towards implementing its SCIP. The SCIP Annual Snapshot includes information on accomplishments, interoperability gaps, as well as current and future strategic initiatives for improving interoperability. Grantees should describe in grant applications how projects align to needs identified in the SCIP, SCIP Annual Snapshot, or other applicable plans.

3.2 Coordinate with Statewide Emergency Communications Leaders

To ensure that projects are compatible, interoperable, and support statewide plans and strategies, grantees should consult the appropriate statewide leaders or entities prior to developing projects for funding. Some Federal programs require or encourage coordination of grant submissions with the SWIC and other statewide leaders (e.g., SPOC, State Emergency Management Agency Director, 911 Administrator, Homeland Security Director), as well as require applicants to attach a letter of project support from these leaders. Grantees should also consult the SIGB or SIEC, as they serve as the primary steering group for the statewide interoperability strategy. Additionally, grantees should consult any subject matter experts serving on governance bodies such as broadband experts, chief information officers, representatives from utilities, or legal and financial experts when developing proposals.

3.3 Recognize Changes in the Emergency Communications Ecosystem

Grantees should understand the more complex and interdependent ecosystem that has emerged due to evolving technologies, risks, stakeholders, and policies impacting many facets of emergency communications including planning, operations, equipment, and training. Key issues impacting Federal emergency communications grants include developments in advanced technologies, national policies and laws, spectrum issues, and the reduction and streamlining of grant programs.

Developments in Advanced Technologies[18]

Traditionally, LMR systems were the primary capabilities the public safety community used to achieve mission critical voice communications. To augment their LMR capabilities, emergency response agencies are increasingly using commercial wireless broadband services and, in some cases, procuring private broadband networks for mission critical data communications. IP-enabled networks stand to transform how public officials will communicate by providing unparalleled connectivity and bandwidth that enhance situational awareness and information sharing. Communication network modernization is also occurring with the migration of the Nation's 911 infrastructure to Next Generation 911, an IP-based model that will enable the transmission of both voice and data (e.g., texts, images, video) to flow seamlessly from the public, through the 911 network and eventually, directly to first responders. Also, the deployment of a nationwide public alerting system is using traditional media, such as broadcast and cable, as well as IP-based technologies to transmit alerts to mobile phones and other devices.

Public safety information technology systems include sensitive data, such as law enforcement information and electronic medical records, which create new security considerations including storage, access, and authentication. While electronic access to this data enables more effective response operations, it also poses risks including system failures, lack of user or server connection, and hostile hackers. As the community adopts new technologies and applications, then it too must increase understanding and planning for the security risks associated with the open architecture and vast complexity of IP-based technologies and services.

To meet these challenges, a multifaceted cybersecurity approach is needed to ensure the confidentiality and the integrity of the communication system and sensitive data. For example, comprehensive cyber training and education will be required on the proper use and security of devices, phishing, malware, and other potential threats. In addition, planning must match user needs against bandwidth requirements and the options for network resiliency. Assessments of cyber risks and strategies to mitigate vulnerabilities must be conducted before the deployment of IP-based networks occurs to ensure that mission requirements can be met securely and reliably from the outset.

The convergence of technologies and risks in this evolving ecosystem shows the importance of ongoing planning for emergency communications. Grantees and their respective governance and leadership must consider all components that support LMR, broadband, cyber, and IP-based technologies as they update strategic plans and common operational protocols that ensure the operability, interoperability, and continuity of emergency communications systems. Additionally, grantees should prioritize maintaining LMR systems and other emergency communications capabilities gained in recent years as they gradually adopt and deploy IP-based technologies and services.

[18] The term "advanced technologies" includes, but is not limited to, the use of emerging technologies to provide advanced interoperability solutions; solutions that allow the use of commercial services, where appropriate, to support interoperable communications; IP-based technologies; use of common advanced encryption options that allow for secure and vital transmissions, while maintaining interoperability; use of standards-based technologies to provide voice and data services that meet wireless public safety service quality; solutions that have an open interface to enable the efficient transfer of voice, data, and video signals; and investments in these technologies, such as NG911 and Bridging System Interface.

National Policies and Laws

In addition to technological developments, the Nation is evolving its approach to preparing for and responding to incidents through the *National Preparedness Goal*, which promotes a shared responsibility across all levels of government, private and nonprofit sectors, and the general public. Applicable plans, laws, and policies include the 2014 NECP, the Middle Class Tax Relief and Job Creation Act, and the Presidential Policy Directive–8 (PPD–8):

- ***National Emergency Communications Plan.*** Released in November 2014, the focus of this updated Plan is to ensure that strategies, resource decisions, and investments for emergency communications keep pace with the evolving environment, and that the emergency response community is collectively driving toward a common end-state for communications. The 2014 NECP provides information and guidance to those that plan for, coordinate, invest in, and use communications to support response and recovery operations.[19]

  Grantees should read the 2014 NECP to understand the national emergency communications strategy, and to ensure that proposed investments support the goals, objectives, and recommendations of the Plan. In addition, grantees are encouraged to review NECP supplemental materials such as assessments, annual progress reports, and implementation documents. Additionally, grantees should work with the SWIC to ensure alignment of the SCIP and other emergency communications plans to the NECP.

- ***Middle Class Tax Relief and Job Creation Act.*** Signed into law on February 2012, the Act established FirstNet, an independent authority within NTIA, and directed it to ensure the building, deployment, and operation of the NPSBN.[20] The Act reallocated and designated D-Block spectrum for public safety use to FirstNet. It also established the State and Local Implementation Grant Program (SLIGP) to assist State, local, tribal, and territorial governments as they plan for the NPSBN.[21] SLIGP is a formula-based, matching grant program administered by the NTIA that has awarded $116.5 million in grants to 54 U.S. states and territories. This funding provides recipients with the resources to work with stakeholders throughout the State or territory to identify needs, gaps, and priorities for public safety wireless broadband. This work will also help recipients prepare for consultation with FirstNet.

  FirstNet is fully engaged in comprehensive outreach and consultation efforts with public safety entities and Federal, state, local, tribal, and territory jurisdictions to plan for the network. FirstNet has actively sought input from industry, states, territories, tribes, first responders, and other stakeholders on what the network should look like, how it should function, and whether and how vendors can meet the technical objectives of the NPSBN. FirstNet is working to identify offerors to assist in building, deploying, and operating the network. Once an offeror is selected, FirstNet will work with the offeror to finalize, among other things, a network architecture, technical and user objectives, spectrum access policies, and deployment plans. While entities may want to pursue funding for

[19] For more information on the NECP, see: http://www.dhs.gov/necp.
[20] For more information on the Act, see: http://www.ntia.doc.gov/category/public-safety.
[21] For information on SLIGP, see: http://www.ntia.doc.gov/other-publication/2013/sligp-federal-funding-opportunity.

broadband equipment and systems, there is limited equipment available currently and such equipment may not comply with FirstNet's final network architecture of the NPSBN. Therefore, at this time, grantees would be best served by acquiring long-term evolution (LTE) network equipment only after receiving further guidance from FirstNet on the technical requirements of the NPSBN and focusing funding on outreach and planning activities (e.g., community outreach and education, documenting user needs) that support statewide planning for the arrival of broadband and other advanced technologies.

Grantees interested in investing Federal funds in broadband-related projects should consult the Federal granting agency to understand all requirements and restrictions impacting broadband investments. Grantees should be aware that FirstNet has only granted Spectrum Management Lease Agreements (SMLA) to five projects for their use of Band 14 spectrum, of which FirstNet is the sole nationwide licensee. FirstNet does not anticipate awarding any more SMLAs prior to the deployment of the NPSBN. Grantees should work closely with the SWIC, statewide emergency communications leaders, and the Federal granting agency to ensure projects remain in compliance with programmatic and technical requirements. Additionally, the Act provides the National Highway Traffic Safety Administration (NHTSA) with $115 million for grants to improve 911 services. Grantees should continue to monitor current Federal actions affecting broadband and 911 programs funded through the Act.[22]

- ***Presidential Policy Directive–8.*** Signed by the President in March 2011, PPD–8, *National Preparedness*, is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation. It consists of four main components: the *National Preparedness Goal*; National Preparedness System; *National Preparedness Report*[23]; and the Campaign to Build and Sustain Preparedness. The directive emphasizes that national preparedness is the shared responsibility of the whole community.[24]

  As a result, many grants that fund emergency communications now require grantees to engage the whole community in planning. FY 2016 Federal grant programs will require grantees to demonstrate how a whole community approach to project planning was used, and explain how core capabilities were improved. Grantees are encouraged to engage their community early in project development to ensure they can provide evidence of community involvement in applications. Engaging the whole community in project planning not only improves preparedness and response, but also strengthens grant applications.

Spectrum Issues

The FCC authorizes State, local, and some tribal public safety entities to use specific spectrum bands to operate emergency communications systems. By statute, FirstNet holds the FCC

[22] Updates on the 911 Grant Program will be posted on the National 911 Program's website at http://www.911.gov/ when funding becomes available.
[23] The FY 2015 *National Preparedness Report* emphasizes the following priorities: Cybersecurity; Infrastructure Systems; Access Control and Identity Verification; Economic Recovery; Housing; and Long-term Vulnerability Reduction.
[24] For more information on PPD-8, see: http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

license for the 700 MHz public safety broadband spectrum to build and operate the NPSBN. Grantees seeking Federal funds for emergency communications projects should be aware that there are several Federal initiatives and actions affecting spectrum use for public safety entities. Grantees should review the following spectrum issues, confirm that their proposed projects are consistent with regulatory requirements and initiatives, and consult the appropriate coordinator (e.g., Frequency Coordinator, SWIC, and/or SPOC), the FCC, and/or FirstNet early in the project development process to determine whether the grantee will have authority to operate in the desired spectrum, once complete. Key spectrum-related issues are described below:

- **Ultra-High Frequency (UHF)/Very High Frequency (VHF) Narrowbanding**.[25] The FCC mandated that all non-Federal LMR licensees operating between 150 and 512 MHz and using 25 kilohertz (kHz) bandwidth voice channels migrate to 12.5 kHz bandwidth or equivalent efficiency by January 1, 2013. Grantees should ensure that existing LMR systems are compliant with these narrowbanding requirements and consult with the SWIC and the FCC on any non-compliance issues to avoid admonishment, monetary fines, or loss of license. Grantees that have not complied with the FCC narrowband mandate may face limitations on their eligibility for Federal funding.[26]

- **700 MHz Narrowbanding**. The FCC has eliminated the requirement for further narrowbanding of 700 MHz public safety narrowband systems from 12.5 kHz down to 6.25 kHz bandwidth.[27]

- **800 MHz Reconfiguration (Rebanding).**[28] In 2004, the FCC ordered the reconfiguration of portions of the 800 MHz band to separate public safety systems from commercial cellular networks and thereby reduce harmful interferences. 800 MHz rebanding is complete in most areas of the U.S. but remains to be completed in the U.S.-Mexico border region. Public safety entities contemplating communication projects in areas still undergoing rebanding should consult the SWIC, the FCC, and the 800 MHz Transition Administrator, which is responsible for overseeing the rebanding process and providing technical assistance to affected licensees.

- **T-Band Migration.** The Middle Class Tax Relief and Job Creation Act of 2012 authorized the future auction of the 470–512 MHz ultra-high frequency band, referred to as the T-Band. Several large urban areas use the T-Band for public safety communications.[29] The Act requires the FCC to commence the auction process within nine years (i.e., by 2021) and requires T-Band public safety licensees to relocate from the T-Band to other, unspecified spectrum, two years after the completion of the auction of this spectrum. In October 2014, the FCC released an order that provides T-Band incumbents that commit to return an equal amount of T-Band channels priority access to

[25] For more information on narrowbanding, see: http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html.
[26] See "Guidance for licensees for FCC's narrowband operation requirement" at: http://www.fcc.gov/document/guidance-licensees-fccs-narrowband-operation-requirement. Grantees with questions on narrowbanding may contact the FCC at: narrowbanding@fcc.gov.
[27] FCC Report and Order 14-172, http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1024/FCC-14-172A1.pdf.
[28] For more information on 800 MHz reconfiguration, see: http://www.800ta.org/.
[29] Entities operating in the T-Band include: Boston (MA), Chicago (IL), Dallas/Ft. Worth (TX), Houston (TX), Los Angeles (CA), Miami (FL), New York City (NY), Philadelphia (PA), Pittsburgh (PA), San Francisco/Oakland (CA), Washington DC/Maryland/Virginia.

the 700 MHz Narrowband Reserve Channels for a five-year period.[30] Grantees seeking funding for relocation of T-Band systems should consult the FCC,[31] SWIC, and a frequency coordinator[32] early in the project development process to ensure the project supports statewide plans for improving emergency communications, and is planned in the appropriate spectrum.

- **700 MHz Public Safety Broadband Spectrum.**[33] The Middle Class Tax Relief and Job Creation Act of 2012 authorized the establishment of the NPSBN, dedicated a block of 700 MHz spectrum for this purpose, and named FirstNet as the single licensee for the spectrum block. Incumbents currently operating in this band may need to migrate from the band to clear the spectrum for NPSBN use as early as 2017. FirstNet has announced that it will establish a grant program to support such relocation by qualified licensees. Grantees operating in the 700 MHz public safety broadband spectrum should consult the SPOC and the SWIC during project development to ensure that projects support the statewide plan for broadband deployment in the 700 MHz public safety broadband spectrum.

In general, grantees should consult with the regulatory agency or with the appropriate State-level points of contact when developing public safety projects to ensure entities are in compliance with Federal spectrum initiatives and regulations, and projects will have authority to operate in the designated spectrum.[34] To assist State, local, tribal, and territorial levels of government, many grants that fund interoperable communications equipment allow grant funds to be used for spectrum-related activities,[35] including:

- Identification, assessment, coordination, and licensing of new spectrum resources
- Development and execution of spectrum migration plans
- Assessment of current communications assets, services, and capabilities
- Training associated with systems migration to new spectrum allocations
- Replacement of non-compliant communications equipment and services
- Acquiring/upgrading tower sites and facilities needed to comply with spectrum migration[36]
- Reprogramming existing equipment to comply with spectrum migration

Reduction and Streamlining of Grants

The elimination and consolidation of grants funding emergency communications over the past several years have increased competition for funding and necessitated increased planning among jurisdictions and disciplines. Emergency communications leaders and agencies are strongly encouraged to work with other jurisdictions and disciplines to coordinate resources and projects and to avoid duplication of activities. Additionally, when developing funding proposals, grantees are advised to work with State-level planning offices to incorporate emergency

[30] For more information, see FCC 14-172 at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-172A1.pdf.
[31] Grantees can contact the FCC Public Safety and Homeland Security Bureau at: pshsbinfo@fcc.gov.
[32] For more information on frequency coordinators, see: http://transition.fcc.gov/pshs/public-safety-spectrum/coord.html.
[33] The public safety broadband spectrum band is 763-768 MHz and 793-798 MHz.
[34] Contact the FCC's Public Safety Homeland Security Bureau at pshsbinfo@fcc.gov and FirstNet at outreach@firstnet.gov.
[35] Generally, Federal licensing fees are *not* allowable under most Federal grants; however, grantees should not anticipate having such expenses as public safety entities are exempt from FCC filing fees. For more information, see: http://transition.fcc.gov/fees/.
[36] Some Federal grants do not allow construction or ground-disturbing activities. Consult the grant officer on these activities.

communications needs into statewide plans and to ensure emergency communications projects are prioritized by States and territories. Grantees are encouraged to:

- Coordinate projects with neighboring jurisdictions and multiple agencies
- Develop regional, multi-jurisdictional, multi-disciplinary, and cross-border projects to not only promote greater interoperability across agencies, but also to pool grant resources, facilitate asset-sharing, and eliminate duplicate purchases[37]
- Leverage assessment data to develop strong statements of need that can be shared with State leaders responsible for prioritizing projects for funding[38]
- Identify additional sources of funding for emergency communications improvements[39]

3.4 Understand Federal Grant Requirements and Restrictions

Federal Grant Requirements

Emergency communications grants are administered by numerous Federal agencies in accordance with various statutory, programmatic, and departmental requirements. Grantees are encouraged to carefully review grant guidance to ensure applications meet all grant requirements, including:

- Program goals
- Eligibility requirements
- Application requirements (e.g., due dates, submission dates, matching requirements)
- Allowable costs and restrictions on allowable costs
- Technical standards preferred, required, or allowed under each program
- Reporting requirements

Additionally, grantees should be aware of common requirements for grants funding emergency communications,[40] including:

- **Environmental Planning and Historic Preservation (EHP) Compliance.** Grantees must comply with all applicable EHP laws, regulations, Executive Orders, and agency guidance. Grantees are strongly encouraged to discuss projects with Federal grant program officers to understand EHP restrictions, requirements, and review processes prior to starting the project.

- **NIMS.** Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, requires the adoption of NIMS to strengthen and standardize preparedness

[37] Grantees should work with SWICs and the FCC to ensure that projects do not interfere with the 800 MHz rebanding effort occurring along the U.S.-Canada and U.S.-Mexico borders. For more information on the rebanding process, see: http://transition.fcc.gov/pshs/public-safety-spectrum/800-MHz/. Grantees are reminded that Federal funding may not be allocated to international entities, unless authorized by law, and placement of Federally-funded equipment on international property may be subject to special terms and conditions. Grantees should work closely with grant officers on these projects.

[38] Grantees are encouraged to use NECP Goal Demonstrations, AARs, and similar assessments to demonstrate where there are gaps in emergency communications, and to appeal to State-level leaders for funding to address those gaps.

[39] For additional sources of funding, see the FY 2015 List of Grants Funding Emergency Communications posted to the SAFECOM website at: http://www.dhs.gov/funding.

[40] While these are common requirements that affect many emergency communications grants, they may not apply to all grants; therefore, grantees should consult their grant guidance and grant officer for specific questions on grant requirements.

response, and to receive preparedness grant funding. State, local, tribal, and territorial grantees should ensure that the most recent NIMS reporting requirements have been met.[41]

- **State Preparedness Report (SPR) Submittal.** Section 652(c) of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109-295), 6 U.S.C. §752(c), requires any State that receives Federal preparedness assistance to submit an SPR to FEMA. Grantees should consult with the SAA to ensure that the most recent SPR has been submitted.

- **Threat and Hazard Identification and Risk Assessment (THIRA).** In FY 2016, DHS is requiring recipients from the Homeland Security Grant Program, Tribal Homeland Security Grant Program, and the Emergency Management Performance Grants Program to complete a THIRA report. The THIRA process helps communities to understand their threats and hazards and how the impacts may vary according to time of occurrence, season, location, and numerous other community factors. The THIRA process results in whole community-informed capability targets and resource requirements necessary to address anticipated and unanticipated risks.[42] Developing and updating an effective THIRA requires active involvement from the whole community to ensure assessments and planning efforts are representative of all needs. Therefore, recipients should actively engage in the THIRA process and convey the impact of various threats and hazards on emergency communications, as well as desired outcomes to statewide THIRA planners. Recipients should be aware that DHS funding may be placed on hold until the THIRA is submitted. For additional information, refer to each grant program's FY 2016 Notice of Funding Opportunity for grant-specific THIRA requirements and impact on annual grant funding.[43]

- **Authority to Operate.** In establishing the NPSBN and providing the spectrum license to FirstNet, Congress required FirstNet to ensure the building, operation, and maintenance of a nationwide interoperable public safety broadband network with a single national architecture to ensure interoperability for public safety entities. FirstNet is the single licensee for the combined public safety broadband spectrum band (763-768 MHz and 793-798 MHz) and D Block spectrum (758-763 MHz and 788-793 MHz), also referred to as Band 14. Grantees that do ***not*** have authority to operate in that designated public safety broadband spectrum (e.g., a spectrum management lease agreement with FirstNet) cannot utilize that spectrum. Grantees that do ***not*** have access to the designated spectrum should not use Federal financial assistance to support acquisition-based or deployment-based broadband projects until such time as they have received the necessary authority to operate in the designated spectrum. Grantees that have authority to operate may submit projects for funding provided that the request is consistent with the lease agreement.

[41] National Integration Center (NIC) has advised State, local, tribal, and territorial governments to self-assess their respective progress relating to NIMS implementation objectives in the NIMS Compliance Assistance Support Tool (NIMSCAST). The list of objectives against which progress and achievement are assessed and reported can be found at: https://www.fema.gov/national-incident-management-system.

[42] For additional information on the THIRA process, refer to Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment Guide at: http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf.

[43] Funding Opportunity Announcements for FEMA preparedness grant programs can be located at: http://www.fema.gov/preparedness-non-disaster-grants.

Grantees should notify FirstNet prior to submitting a funding application and be aware that their project will be subject to Federal review to ensure proposed projects support FirstNet's efforts to deploy the NPSBN.

- **Reporting.** Federal agencies are improving how they demonstrate the impact and effectiveness of Federal grant programs.[44] As a result, grantees may be required to report project-level information, performance measurement data, detailed financial reports, and progress reports. Grantees are encouraged to use existing documentation and data (e.g., SCIPs, AARs, assessments) to help measure performance and demonstrate how gaps in capabilities will be/were addressed through the use of Federal grant funding. Grantees are strongly encouraged to:
  - Develop performance measures at the start of the grant
  - Include interval performance measures and milestones to gauge project progress
  - Track performance and report the impact of funds on emergency communications
  - Include metrics on improvements in interval and final grant reports

Grantees should ensure that all grant requirements are met and that they can implement the project as proposed and within the grant period of performance; properly manage grant funding; fulfill grant reporting requirements; and comply with Federal grant restrictions.

Federal Grant Restrictions

Grantees should be aware of common restrictions on Federal grant funding and should consult the grants officer with any questions, particularly as requirements vary by program.

- **Commingling or Duplication of Funds.** Since multiple agencies are involved in communications projects, projects are often funded with multiple grant programs, creating a risk of commingling and duplication. Grantees must ensure that Federal funds are used for purposes that were proposed and approved, and have financial systems in place to properly manage grant funds. Grantees cannot commingle Federal sources of funding. The accounting systems of all grantees and sub-grantees must ensure that Federal funds are not commingled with funds from other awards or Federal agencies.

- **Cost Sharing/Matching Funds.** Grantees must meet all matching requirements prescribed by the grant. If matching funds are required under a grant, grantees must provide matching funds or in-kind goods and services that must be:
  - Allowable under the program and associated with the investment
  - Applied only to one Federal grant program
  - Valued at a cost that is verifiable and reasonable
  - Contributed from non-Federal sources
  - Treated as part of the grant budget
  - Documented the same way as Federal funds in a formal accounting system

[44] See the Government Accountability Office's report on duplication at: http://www.gao.gov/products/GAO-12-342SP.

- **Funding and Sustaining Personnel.** In general, the use of Federal grant funding to pay for staff regular time is considered personnel and is allowable. Grantees are encouraged to develop a plan to sustain critical communications positions in the event that Federal funds are not available to support the position in future years. For more information on personnel, refer to Section 4. *Eligible Activities – Personnel.*

- **Supplanting.** Grant funds cannot supplant (or replace) funds previously funded or budgeted for the same purpose. Most Federal grants funding emergency communications restrict grantees from hiring personnel for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities.

4. Eligible Activities

The following section details eligible emergency communications activities commonly funded by Federal grants, including personnel and the four common cost categories: Planning and Organization, Training, Exercises, and Equipment.[45] Grantees seeking to improve interoperable emergency communications are encouraged to allocate grant funding to these activities but must consult the specific grant guidance for allowable costs.

The intent of this section is to raise awareness as to the types of costs that can be covered under most Federal grants funding emergency communications. Grantees should note, however, that all activities listed may not be eligible for funding under all grant programs. Grantees should read each grant guidance and related information carefully to ensure that activities proposed are eligible under the program before developing or submitting applications.

4.1 Personnel

Many Federal grants allow grantees to hire full- or part-time staff, contractor staff, or consultants to assist with emergency communications planning, training, and exercise activities.[46] Allocating funding toward personnel helps ensure that grants and grant-funded projects are managed, that State-level planning meetings are attended, that emergency communications needs are represented, and plans are completed. Personnel can be hired to develop and conduct training and exercises, and to complete AARs.

Eligible Personnel Costs

- **Personnel to assist with planning.** Full- or part-time staff, contractors, or consultants may be hired to support emergency communications planning activities, including:
  - Statewide, local, tribal, territorial, or regional interoperability coordinator(s)
  - Project manager(s)
  - Program director(s)
  - Emergency communications specialists (e.g., frequency planners, radio technicians, cybersecurity)

- **Personnel to assist with training.** Full- or part-time staff, contractors, or consultants may be hired to support emergency communications training activities, including personnel who can:
  - Assess training needs
  - Develop training curriculum
  - Train the trainers
  - Train emergency responders
  - Develop exercises to test training
  - Support training conferences

[45] The general cost categories for grants include: Planning, Organization, Equipment, Training, and Exercises (POETE). Some grants do not provide a category for Organizational costs, but allow organizational costs to be included under the Planning cost category. Grantees should be aware that emergency communications personnel, planning, and organizational costs are often allowable under the Planning cost category for grants.

[46] Typically, the use of Federal grant funding to pay for staff or contractor regular time is considered personnel.

  - Develop and implement a curriculum covering technical issues raised by broadband and other advanced technologies
  - Serve as subject matter experts (e.g., environmental engineers, grant administrators, financial analysts, accountants, attorneys)

- **Personnel to assist with exercises.** Full- or part-time staff, contractors, or consultants may be hired to support exercises. This includes personnel that will:
  - Assess needs
  - Plan and conduct exercises in accordance with NIMS and the Homeland Security Exercise and Evaluation Program (HSEEP)
  - Implement NECP goal measurements and assessments
  - Lead After Action Conferences and prepare AARs

Additional Requirements and Recommendations for Personnel Activities

Grantees should be aware of common restrictions on Federal grant funding for emergency communications personnel.

- **Sustaining Grant-Funded Positions.** Grantees should ensure that funding for critical communications positions is sustained after the grant period of performance has ended to ensure core capabilities are maintained.

- **Overtime.** Some Federal grants permit the use of funds for overtime related to training. These expenses are limited to the additional costs that result from personnel working more than 40 hours per week as a direct result of their attendance at approved activities (e.g., emergency communications training and exercises).

- **Backfill-related Overtime.** Some Federal grants allow funds to be used for backfill related overtime. These expenses are limited to costs of personnel who work overtime to perform the duties of other personnel who are temporarily assigned to grant-funded activities (e.g., to attend approved, grant-funded emergency communications training or exercises). These costs are calculated by subtracting the non-overtime compensation, including fringe benefits of the temporarily assigned personnel, from the total costs for backfilling the position. Grantees should ensure that grant funds can be used for overtime and should consult their grant officer to ensure that overtime costs are correctly calculated.

4.2 Planning and Organization

Allocating grant funding for planning helps entities identify and prioritize needs, define capabilities, update preparedness strategies, refine communications plans, identify where resources are needed most, and deliver preparedness programs across multiple jurisdictions, disciplines, and levels of government. Grant recipients are strongly encouraged to assess needs before planning projects, and to carefully plan projects before purchasing equipment.

Eligible Planning and Organization Costs

- **Development or enhancement of interoperable emergency communications plans**. Grant funds may be used to develop or enhance interoperable communications plans and align plans to the strategic goals, objectives, and recommendations set forth in the NECP. Examples of emergency communications plans include:
  - Plans to implement and measure the NECP
  - SCIPs and SCIP Annual Snapshots
  - Tactical Interoperable Communications Plans (TICP) or other regional interoperable emergency communications plans
  - Disaster emergency communications plans
  - Communications system life cycle planning, including migration planning
  - Plans for narrowband conversion and compliance
  - Plans for 800 MHz rebanding
  - Plans for relocating existing systems operating in the T-Band
  - Stakeholder statements of need and concept of operations (CONOPS)
  - As-is and proposed enterprise architectures
  - System engineering requirements
  - Acquisition planning for the procurement of systems or equipment
  - Planning for backup communications in the event that primary systems or equipment fail (e.g., contingency and strategic planning)
  - Planning for training and exercises
  - Planning activities in support of the NPSBN
  - Planning activities for cybersecurity
  - Planning activities for 911

- **Engagement of Federal, State, local, tribal, territorial, private, and public sector entities in planning.** Many Federal grants require engagement of the whole community in planning to adequately assess and address needs, and to implement the National Preparedness System. The *National Preparedness Goal* and the National Preparedness System concepts, as described in PPD–8 recognize that the development and sustainment of core capabilities are not exclusive to any single level of government or organization, but rather require the combined effort of the whole community.[47] As a result, the following activities are often supported through Federal grants funding emergency communications:
  - Conducting conferences and workshops to receive input on plans
  - Meeting expenses related to planning
  - Public education and outreach on planning
  - Travel and supplies related to planning or coordination meetings
  - Attending planning or educational meetings on emergency communications

- **Establishment or enhancement of interoperability governing bodies.** Strong governance structures and leadership are essential to effective decision-making, coordination, planning for, and managing emergency communications initiatives. Grant funds may be used to establish, update, or enhance statewide, regional (e.g., multi-State,

[47] Core capabilities include Prevention, Protection, Mitigation, Response, and Recovery, and are further defined in the *National Preparedness Goal* on the FEMA website at: http://www.fema.gov/preparedness-1/national-preparedness-goal.

multi-urban area), or local interoperability governing bodies. Eligible activities may include:

- Developing Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA) to facilitate participation in planning and governance activities
- Meeting or workshop expenses associated with receiving input on plans or supporting a funded activity
- Increasing participation in governing bodies through public education and outreach
- Travel and supplies for governing body meetings
- Attending planning or educational meetings on emergency communications or public safety broadband issues
- Developing SOPs and other templates to provide access to and use of existing resources and infrastructure
- Establishing new bodies or sub-groups to address broadband planning
- Ensuring coordination between traditional LMR governance programs and other decision-making offices, bodies, and individuals that oversee new technology deployments in States, territories, localities, and tribes

- **Development of emergency communications assessments and inventories**. Grantees are encouraged to allocate grant funding to planning activities, such as assessments of:
  - Technology capabilities, infrastructure, and equipment (e.g., CASM NextGen, fleet maps)
  - SOPs, coordination of interoperability channels, and regional response plans
  - Training and exercises
  - Narrowband compliance capabilities, assets, and coverage gaps
  - Current broadband usage and user needs
  - Development of cost maintenance models for equipment and usage

- **Development or enhancement of interoperable emergency communications protocols.** Funds may be used to enhance multi-jurisdictional and multi-disciplinary common planning and operational protocols, including the development or update of:
  - SOPs, shared channels and talk groups, and the elimination of coded substitutions (i.e., developing and implementing common language protocols)
  - Partnership agreements, MOUs, and cross-border agreements
  - Plans to integrate SOPs across disciplines, jurisdictions, levels of government, and with private entities, as appropriate, and into mutual aid agreements
  - Response plans to specific disasters or emergencies
  - Field guides and templates for field guides

- **Planning activities for emerging technologies.** Grant funds may be used to begin planning for broadband and other advanced technologies. Activities may include:
  - Defining user needs
  - Updating SCIPs to incorporate high-level goals and initiatives, and development of comprehensive plans
  - Developing plans and collecting data in response to broadband requirements issued by FirstNet (e.g., migration plans, contingency plans, feasibility studies)[48]

[48] Development of these plans will not be funded until FirstNet issues guidance on the technical requirements of the network.

  - Preliminary planning for other advanced technologies (e.g., alerts and warnings, Next Generation 911)
  - Conducting assessments of cyber risks and strategies to mitigate vulnerabilities must be conducted before the deployment of IP-based networks

- **Use of priority service programs.** Grant funds may be used to assist priority service planning and engineering, and to facilitate participation in a number of Federal priority service programs,[49] including:
  - Telecommunications Service Priority (TSP)
  - Government Emergency Telecommunications Service (GETS)
  - Wireless Priority Service (WPS)

- **Use of notifications and alerts and warning.** Grant funds may be used to connect with national-level communications systems, including the Integrated Public Alert and Warning System (IPAWS),[50] which consists of:
  - Emergency Alert System
  - Wireless Emergency Alerts
  - IPAWS All-Hazards Information Feed
  - National Oceanic and Atmospheric Administration Weather Radio All Hazards

Additional Requirements and Recommendations for Planning Activities

Additional activities in support of Federal planning initiatives and grant requirements include updating and submitting a SPR, THIRA, and SCIP Annual Snapshot, as well as ensuring NIMS compliance.

4.3. Training

Eligible Training Costs

Recipients are encouraged to allocate Federal grant funds to support emergency communications and incident response training. Communications-specific training activities should be incorporated into statewide training and exercise plans and be reflected in SCIP Annual Snapshots. Recipients should continue to train on LMR systems as it is necessary to ensure that public officials can achieve mission critical voice communications. However, as other communications technologies become integrated into response operations, the need for training becomes even more critical to ensure that response personnel are maximizing the benefits that these new communications capabilities provide. Training projects should be consistent with the NECP priorities and address gaps identified through SCIPs, TICPs, AARs, and other assessments. Training helps to ensure that personnel are familiar with SOPs and equipment, and that equipment is operational. Grantees are strongly encouraged to include training in projects that involve the development of new SOPs or the purchase of new equipment.

[49] For more information on priority services, see: http://www.dhs.gov/gets.

[50] The *2016 IPAWS Supplemental Guidance on Public Alert and Warning* provides guidance on eligible public alert and warning activities and equipment standards for state, local, territory, and tribal prospective recipients. For more information on the IPAWS, see: https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/1413559956428-6f79b8f6e7886041aa5f2338d22a6a8c/FY%202015%20IPAWS%20Supplemental%2010%2002%202014_508.pdf.

- **Development, delivery, attendance, and evaluation of training.**[51] Grant funds may be used to plan, attend, and conduct communications-specific training workshops or meetings to include costs related to planning, meeting space, and other logistics costs, facilitation, travel, and training development. Communications-specific training should focus on:
    - Use of SOPs and other established operational protocols (e.g., common language)
    - NIMS/ICS training
    - COML, COMT, or ICS Communications Unit position training
    - Training in the use of equipment and advanced data capabilities (e.g., voice, video, text)
    - Disaster preparedness training
    - Peer-to-peer training
    - Regional (e.g., multi-State, multi-urban area) training
    - Training associated with narrowband conversion
    - Training related to the broadband planning process
    - Cyber training and education on the proper use and security of devices and applications, phishing, malware, other potential threats, and how to stay on guard against attacks

- **Expenses related to training.** Many Federal grants allow funds to be used for expenses related to training, including:
    - Travel related to training
    - Public education and outreach on training opportunities
    - Supplies related to training (e.g., signs, badges, materials)

Additional Requirements and Recommendations for Training Activities

Grantees should target funding toward certified emergency communications activities, including:

- **Compliance with NIMS.**[52] State, local, tribal, and territorial entities must adopt NIMS as a condition of many Federal grants. Given that the implementation of NIMS requires certain training courses, grantees may target grant funding towards NIMS-compliant training.

- **Completion of Communications Unit Leader Training.** OEC, in partnership with OIC, FEMA, the NIC, and practitioners from across the country, developed performance and training standards for the All-Hazards COML and formulated a curriculum and comprehensive All-Hazards COML Course. Grantees should target grant funding toward this critical training to improve on-site communications during emergencies, as well as satisfy NIMS training requirements.

[51] DHS training catalogs are available at: https://www.firstrespondertraining.gov/odp_webforms/. The Federal-sponsored course catalog can be found at: https://www.firstrespondertraining.gov/webforms/pdfs/fed_catalog.pdf, and the State-sponsored course catalog at: https://www.firstrespondertraining.gov/webforms/pdfs/state_catalog.pdf.

[52] NIMS is a national framework for response, that requires State, local, tribal, and territorial stakeholders to adopt a national ICS, complete certified training, and integrate the framework into State and local protocols. For more information on NIMS training, see: http://www.fema.gov/national-incident-management-system.

4.4 Exercises

Exercises should be used to both demonstrate and validate skills learned in training and to identify gaps in capabilities. To the extent possible, exercises should include participants from multiple jurisdictions, disciplines, and levels of government and include emergency management, emergency medical services, law enforcement, interoperability coordinators, public health officials, hospital officials, and other disciplines and private sector entities, as appropriate. Findings from exercises can be used to update programs to address gaps in emergency communications as well as emerging technologies, policies, and partners. Recipients are encouraged to increase awareness and availability of emergency communications exercise opportunities across all levels of government.

Eligible Exercise Costs

- **Design, development, execution, and evaluation of exercises.** Grant funds may be used to design, develop, conduct, and evaluate interoperable emergency communications exercises, including tabletop and functional exercises. Activities should focus on:
    - Using new or established operational protocols
    - Using interoperable emergency communications equipment
    - Designing and executing exercises of the new equipment purchased to facilitate the conversion process to narrowband, or serving as a strategic technology reserve
    - Designing and executing regional (e.g., multi-State, multi-urban area) exercises
    - Using broadband equipment and systems, and other advanced technologies
    - Testing SOPs

- **Expenses related to exercises.** Many Federal grants allow funds to be used for expenses related to exercises, including:
    - Meeting expenses related to planning or conducting exercises
    - Public education and outreach related to exercises
    - Travel and supplies related to exercises

Additional Requirements and Recommendations for Exercise Activities

Grantees should target funding toward Federal exercise initiatives, including participation in the communications components of the National Level Exercises and the following:

- **Management and execution of exercises in accordance with HSEEP.** The HSEEP Library provides guidance for exercise design, development, conduct, and evaluation of exercises, as well as sample exercise materials. *HSEEP Volume V: Prevention Exercises*, provides recommendations for designing, developing, conducting, and evaluating prevention-focused exercises. The HSEEP Library can be found at: https://hseep.dhs.gov.

- **Compliance with NIMS.** HSPD-5 requires all Federal departments and agencies to adopt NIMS and to use it in their individual incident management programs and activities, including all preparedness grants. Grantees should review the NIMS

requirements at: http://www.fema.gov/emergency/nims/index.shtm, and ensure that all Federally-funded training and exercise activities are NIMS-compliant.

- **Coordination with State-level partners.** Communications-specific exercise activities should be coordinated with the SIGB or SIEC and SWIC to facilitate participation by the appropriate entities (e.g., public safety, utilities, private sector, Federal agencies) and resources (e.g., deployable assets).

4.5 Equipment

Emergency response providers must regularly maintain communications systems and equipment to ensure effective operation, as well as upgrade their systems when appropriate. Grantees are strongly encouraged to invest in standards-based equipment that supports statewide plans for improving emergency communications and interoperability among systems.

- **Design, construction,[53] implementation, enhancement, replacement, and maintenance of LMR and other emergency communications systems and equipment,[54] including:**
  - System engineering requirements
  - As-is and proposed enterprise architectures
  - Development of interoperability verification and validation test plans
  - Development of system life cycle plans
  - Analysis and monitoring of cybersecurity risks
  - Migration to approved, open-architecture, standards-based interoperable technologies
  - Leveraging existing and other advanced technologies (e.g., multi-band/multi-mode capable radio) to expand and integrate disaster communications capabilities among emergency response providers
  - Project management costs associated with equipment and systems
  - Procurement of technical assistance services for management, implementation, and maintenance of communications systems and equipment
  - Reimbursement of cellular and satellite user fees when used for backup emergency communications[55]

- **Use of narrowband equipment.** The FCC mandated that all non-Federal public safety land mobile licensees operating between 150-512 MHz and using 25 kHz channel bandwidth in their radio systems migrate to 12.5 kHz channels by January 1, 2013. As of October 17, 2014, the FCC eliminated a second narrowbanding mandate, which required 700 MHz public safety licensees to migrate from a 12.5 kHz voice efficiency standard to a 6.25 kHz voice efficiency standard by December 31, 2016. Grantees should ensure

[53] Not all Federal grants permit construction-related activities. Consult the grant officer to determine whether construction activities are allowed. For grants that support construction-related activities, see EHP requirements that apply to select construction-related activities in this guidance.

[54] While the activities listed are generally allowable for traditional LMR investments, these activities may be restricted for broadband-related investments. Grantees are strongly encouraged to consult their Federal granting agency before developing broadband proposals for funding to determine if those activities are allowable under the grant.

[55] Many public safety entities use commercial services to augment emergency communications. Reimbursement of cellular and satellite fees are often allowable under Federal grants.

existing systems are compliant and prioritize grant funding, where allowable, toward the following:
  - Replacing non-compliant equipment
  - Acquiring/upgrading additional tower sites to maintain coverage after conversion
  - Reprogramming existing equipment to operate in compliance with the FCC's rule

- **Site upgrades for LMR and other emergency communications systems.**[56]
  - Installing or expanding battery backup, generators, or fuel systems
  - Evaluating existing shelter space for the inclusion of new communications equipment
  - Conducting tower loading analysis to determine feasibility of supporting new antennas and equipment
  - Analyzing site power and grounding systems to determine upgrades needed to support additional communications equipment
  - Analyzing physical site security provisions to determine upgrades and enhancements (e.g., fences, lighting, alarms, cameras, shelter access hardening, physical protective measures)
  - Evaluating Public Safety Answering Points and other 911 infrastructure sites to determine hardware and software upgrades

- **Upgrading connectivity capabilities for LMR and other emergency communications systems.**
  - Documenting existing wireline and wireless backhaul resources to determine used and excess capacity (e.g., connectivity type of either fiber, wireline, or cable at communications sites and existing public safety facilities)
  - Analyzing existing IP backbone to determine gaps in supporting high bandwidth public safety communications system access and applications
  - Planning and modeling network capacity to ensure backhaul links and aggregation points are appropriately provisioned
  - Upgrading existing backbone to support advanced capabilities (e.g., multi-protocol line switching)
  - Installing fiber optic connections and microwave connectivity to support enhanced communications and networking capabilities
  - Assessing and documenting the usage of wireless communications capabilities including:
    - Mobile data systems facilitated through government-owned or commercial services
    - Applications
    - Devices or platforms supported
    - Speed/capacity
    - Accessible data
    - Redundancy and resiliency of systems or services
    - Cost of services and systems

[56] While the activities listed are generally allowable for traditional LMR investments, these activities may be restricted for broadband-related investments. Grantees are strongly encouraged to consult their Federal granting agency before developing any broadband-related proposals for funding to determine if those activities are allowable under the grant.

  - Existing gaps in capabilities, connectivity, coverage, or application support

- **Purchase of:**
  - Standards-based interoperable communications equipment listed on the Authorized Equipment List[57]
  - Equipment that will facilitate the transition of existing systems from the T-Band to authorized spectrum
  - Ancillary equipment to facilitate planning and implementation of interoperable public safety grade communications systems and capabilities (e.g., radio frequency and network test equipment including handheld spectrum analyzers, cable testers)

Additional Requirements and Recommendations for Equipment Purchases

Grantees should anticipate additional requirements when purchasing equipment with Federal grant funds, including:

- **Coordination with statewide emergency communications leaders.** Grantees are strongly encouraged to coordinate with emergency communications governance and leadership, and other State, local, tribal, and territorial partners to ensure consistency with statewide plans, and compatibility among existing and proposed emergency communications systems.

- **Compliance with SAFECOM technical standards.** Grantees must ensure that all grant-funded equipment complies with the SAFECOM technical standards in Appendix B of this Guidance, unless otherwise noted in a program's grant guidance.[58] Many Federal grants require grantees to explain how their procurements will comply with the applicable standards for LMR, IP-based systems, or alerts and warning or provide compelling reasons for using non-standards-based solutions. Grantees should document all purchases and evidence of compliance with standards-based requirements.

- **Compliance with FCC Requirements.** Grantees are encouraged to consult with the FCC during application development to determine whether projects will be able to access the appropriate spectrum for its planned operations or if a waiver is needed. Grantees can contact the FCC at PSHSBinfo@fcc.gov.

- **Compliance with Federal EHP laws and policies.** Grantees must ensure that Federally-funded projects comply with relevant EHP laws. The installation of communications towers and other ground-disturbing activities frequently requires EHP review. Each agency (and sometimes each program) has its own EHP compliance process. Grantees should discuss proposed construction-related activities with Federal granting agencies

[57] For a list of equipment typically allowed under FEMA grants, see: http://www.fema.gov/authorized-equipment-list.
[58] Technical standards and requirements vary among Federal grant programs (especially grants funding research and testing). Applicants should review grant guidance to ensure that specific standards, terms, and conditions under the grant are met. DHS FEMA grant recipients must adhere to compliance requirements specified in SAFECOM Guidance Appendix D.

before beginning work to determine whether proposed activities are allowed, and to determine if proposed activities are subject to EHP review.[59]

- **Adoption of new technologies.** Grantees are encouraged to migrate to approved, open architecture and to leverage existing and other advanced technologies (e.g., multi-band/multi-mode capable radio) to expand and integrate disaster communications capabilities among emergency response providers.

- **Sustainment of current LMR capabilities.** Grantees are strongly encouraged to sustain current LMR capabilities to sustain mission critical voice capabilities, as well as to ensure their LMR systems continue to deliver reliable communications.[60]

- **Compliance with Federal procurement requirements.** As a condition of funding, recipients agree to comply with Federal procurement requirements. Grantees are responsible for ensuring open and competitive procurements, subject to the specific requirements of the grant program, and applicable State or local procurement requirements. Grantees are required to have written procurement policies in place, are encouraged to follow the same policies and procedures it uses for procurement from its non-Federal funds, and should include any clauses required by the Federal Government. The following are key procurement tenets when using Federal funds:
  - Procurement transactions should be conducted to ensure open and free competition
  - Grantees/sub-grantees should avoid non-competitive practices (e.g., contractors that developed the specifications for a project should be excluded from bidding)
  - Grantees/sub-grantees may not supplant, or replace, non-Federal funds that are already budgeted or funded for a project

- **Promotion of regional capabilities.** Grantees should coordinate and collaborate with agencies from neighboring States and regions to facilitate regional operable and interoperable solutions, including shared solutions.

- **Development of communications system life cycle plans.** Emergency response providers must upgrade and regularly maintain communications systems to ensure effective operation. Some programs require grantees to submit system life cycle plans for equipment purchased with Federal grant funds.[61] As a result, grantees should develop a system life cycle plan for any communications system.

- **Understanding of cost share**. Federal grants often require recipients to provide a percentage of total costs allocated to equipment. Federal funds cannot be matched with other Federal funds, but can be matched through State, local, tribal, or territory cash and in-kind contributions. Match requirements are often waived for ancillary territories.

[59] To learn more about Federal EHP requirements, see the Council on Environmental Quality Regulations, 40 CFR Part 1500-1508, or the U.S. Department of Energy website at: http://ceq.hss.doe.gov/nepa/regs/ceq/toc_ceq.htm.
[60] For guidance on funding and sustainment of LMR capabilities, see: http://www.dhs.gov/safecom/funding.
[61] For guidance on system life cycle planning, see: http://www.dhs.gov/safecom/resourceslibrary.

5. Emergency Communications Systems and Capabilities

Emergency communications are accomplished through many technologies, each with varying capabilities, standards, and features. As the public safety community adopts new technologies, it is important to recognize that LMR will remain the primary tool for mission critical voice communications for many years to come. This convergence requires a multi-path approach in maintaining LMR systems' operability and interoperability while planning and deploying new emergency communications technologies. As such, grantees should invest in sustaining LMR capabilities while also planning for new technologies.

As LMR and IP-based technologies continue to converge with one another, interoperability and cybersecurity become increasingly important. When procuring equipment or software for emergency communications systems, grantees should purchase standards-based technologies to facilitate interoperability and security among jurisdictions and disciplines at all levels of government. Table 2 provides best practices for promoting interoperability and security in several types of emergency communications capabilities. For detailed standards and resources for each system type, refer to Appendix B.

Table 2. Best Practices when Purchasing Emergency Communications Capabilities

Systems	Best Practices
Land Mobile Radio (LMR)	• Review the P25 technical standards for LMR • Include P25 in Statement of Requirements and vendor inquiries • Select P25 eligible equipment • Obtain documented evidence of P25 compliance • Ensure additional features purchased are P25-compliant • Ensure non-standard features are identified and understand impact on interoperability • Provide written justification required for non-P25 purchases
Next Generation 911 (NG911)	• Read the *NG911 Standards Identification and Review*[62] and select a Standard Development Organization's standards • Consult with the National 911 Program Office regarding any updated standards • Select IP-enabled 911 open standards equipment and software
Public Safety Broadband	• Consult with the FirstNet SPOC for the latest guidance from FirstNet and determine if the proposed project is consistent with State planning efforts • Identify the authority to operate on public safety spectrum through the FirstNet SPOC; if lease agreement is not in place, target funding toward planning and outreach activities; if lease agreement is in place, contact FirstNet to ensure the proposed project is consistent with lease terms • Conduct and plan site and backhaul upgrades as well as software and IT infrastructure upgrades for connectivity capabilities necessary to connect to NPSBN • Delay purchase of LTE equipment until further guidance from FirstNet is available
Data Information Sharing	• Read the Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data eXchange Language (EDXL) and National Information Exchange Model (NIEM) resources on data messaging standards • Read the standards, guides, and best practices provided by the Information Sharing Environment (ISE) initiative[63]
Alerts and Warnings	• Read the IPAWS Toolkit for Alerting Authorities • Consult with IPAWS Program Office for best practices and compatible applications • Ensure compliance with Common Alerting Protocol (CAP) and IPAWS Profile[64]

[62] For a copy of the *NG911 Standards Identification and Review*, see: http://www.911.gov/911-issues/standards.html.
[63] For more information on the ISE initiative, see: https://www.ise.gov/resources/standards-guides-best-practices.
[64] For information on CAP and IPAWS, see: https://www.fema.gov/integrated-public-alert-warning-system.

6. Grants Management Best Practices

The proper management of grants enables grantees to effectively implement projects and access grant funds. It also can establish the entity as a trusted and capable steward of Federal funding that is able to manage additional funds in the future. This section provides guidance and best practices for grantees to use throughout the grant life cycle. Table 3 provides best practices during the four major phases of the grant:

- Planning grant applications (Pre-Award)
- Managing grant funding (upon Award)
- Implementing grant-funded projects (Post Award)
- Completing Federal grant projects (Closeout)

Table 3. Suggested Actions and Best Practices to Use during Grant Cycle Phases

Phases	Suggested Actions/Best Practices
Pre-Award	• Review and understand the NECP, SCIP, and other applicable plans • Coordinate with key governance and leadership to document needs, align projects to plans, and identify funding options • Work with SAA to include projects in State preparedness plans and to secure funding • Review grant requirements included in grant guidance • Consult the Federal granting agency, spectrum authority (i.e., FCC or FirstNet), and *SAFECOM Guidance* when developing projects • Align projects to Federal and State-level plans and initiatives • Include coordination efforts with the whole community in applications • Identify staff to manage financial reporting and programmatic compliance requirements • Develop project and budget milestones to ensure timely completion • Identify performance measures and metrics that will help demonstrate impact • Consider potential impacts of EHP requirements on implementation timelines • Ensure proper mechanisms are in place to avoid commingling and supplanting of funds • Evaluate the ability of sub-grantees to manage Federal funding • Consider how the project will be sustained after grant funding has ended
Award	• Review award agreement to identify special conditions, budget modifications, restrictions on funding, pass-through and reporting requirements, and reimbursement instructions • Update the proposed budget to reflect changes made during review and award • Inform sub-recipients of the award and fulfill any pass-through requirements
Post Award	• Establish repository for grant file and related data to be collected and retained from award through close-out, including correspondences, financial and performance reports, project metrics, documentation of compliance with EHP requirements and technology standards • Ensure fair and competitive procurement process for all grant-funded purchases • Understand the process for obtaining approval for changes in scope and budget • Adhere to proposed timeline for project and budget milestones; document and justify any delays • Leverage Federal resources, best practices, and technical assistance • Complete financial and performance reports on time • Draw down Federal funds as planned in budget milestones or in regular intervals
Closeout	• Complete projects within grant period of performance • Maintain and retain data as required by the award terms and conditions • File close-out reports; report on final performance

7. Funding Sources

Grantees should consider many sources for grant funding information, including traditional grants that have been used to improve emergency communications, as well as other sources of funding that may partially fund emergency communications projects.

Traditional Grant Funding

OEC is charged with coordinating Federal grants funding emergency communications. Through its work with the Emergency Communications Preparedness Center Grants Focus Group, OEC identified 21 Federal grants and loans that fund emergency communications.[65] When applying for these funds, grantees are encouraged to:

- Identify current grant funding available and alternative sources of funding
- Review eligibility requirements, program goals, and allowable costs
- Understand what past grants have funded in your jurisdiction
- Partner with entities eligible to receive other sources of funding

Other Sources of Federal Funding

While the *SAFECOM Guidance* has traditionally covered Federal grant programs, there are other grant and loan programs that can provide extensive funding for State, local, tribal, and territorial public safety communications needs. For example, the USDA Rural Utility Service's integrated interoperable emergency communications and 911 upgrade authority in its Telecommunications Loan Program, and loans and grants from USDA Rural Development's Community Facilities Program have provided critical funding for emergency communications projects.[66]

OEC has included loans in the list of grants posted to the SAFECOM website.[67] Grantees should be aware of the different requirements between grants and loans. Grantees should work with State, local, tribal, and territorial public safety and financial representatives to understand loan requirements and to ensure their proposals meet all requirements under each program.

Also, there are several Federal programs that are not solely focused on public safety communications but have proven to be useful for enhancing public safety communications (e.g., Rural Telecommunications and Rural Electrification Programs). These programs can improve access to 911 services; provide all hazards warnings; improve integration and interoperability of emergency communications; provide critical infrastructure protection and outage prevention; and increase the reliability of standby power to emergency responders. Grantees are encouraged to identify additional sources of funding, such as rural grants and loans, and work with eligible entities for those programs to improve communications infrastructure.

[65] For an updated list of Federal grants and loans that fund emergency communications, see: http://www.dhs.gov/funding. Grantees can find and search grants and loans at: http://www.grants.gov.
[66] For additional information on USDA's Rural Utility Service, refer to: http://www.rurdev.usda.gov/utilities_LP.html.
[67] For a list of grants funding emergency communications, see: http://www.dhs.gov/funding.

Appendix A – Acronym List

3GPP	Third Generation Partnership Project
AAR	After-Action Report
AEL	Authorized Equipment List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BSI	Bridging Systems Interface
BTOP	Broadband Technology Opportunity Program
CAP	Common Alerting Protocol
CASM NextGen	Next Generation Communication Assets Survey and Mapping
CDM	Continuous Diagnostics and Mitigation
CJIS	Criminal Justice Information Services
CEQR	Council on Environmental Quality Regulations
CNSS	Committee on National Security Systems
COML	Communications Unit Leader
COMT	Communications Technician
CONOPS	Concept of Operations
CSIRT	a Computer Security Incident Response Team
CSRIC	Communications Security Reliability and Interoperability Council
CSSP	Communications Sector-Specific Plan
DE	Distribution Element
DES-OFB	Data Encryption Standard-Output Feedback
DHS	Department of Homeland Security
EAS	Emergency Alert System
ECPC	Emergency Communications Preparedness Center
EDXL	Emergency Data eXchange Language
EHP	Environmental and Historic Preservation
EO	Executive Order
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission

FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FirstNet	First Responder Network Authority
FY	Fiscal Year
GETS	Government Emergency Telecommunications Service
HAVE	Hospital Availability Exchange
HF	High Frequency
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
IB	Information Bulletin
ICS	Incident Command System
IDS	Intrusion Detection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEP	Information Exchange Package
IEPD	Information Exchange Package Documentation
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPS	Intrusion Prevention
IS	Independent Study
ISE	Information Sharing Environment
ISO	International Organization for Standardization
ISSI	Inter Radio Frequency Sub-System Interface
IT	Information Technology
ITU	International Telecommunications Union
kHz	kilohertz
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MHz	Megahertz
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
NASNA	National Association of State 911 Administrators
NCCIC	National Cybersecurity and Communications Integration Center
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NENA	National Emergency Number Association
NEP	National Exercise Program
NERC	North American Electric Reliability Corporation
NG-SEC	NENA Security for NG911 Standard
NIFOG	National Interoperability Field Operations Guide
NG911	Next Generation 911
NIC	National Integration Center
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIMSCAST	NIMS Compliance Assistance Support Tool
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Reports
NOAA	National Oceanic and Atmospheric Administration
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OEC	Office of Emergency Communications
OIC	Office for Interoperability and Compatibility
OMB	Office of Management and Budget
P25	Project 25
P25 CAP	P25 Compliance Assessment Program
PMO	Project Management Office
POETE	Planning, Organization, Equipment, Training, and Exercises
PPD	Presidential Policy Directive

PSAP	Public Safety Answering Point
PSCR	Public Safety Communications Research
PSHSB	Public Safety & Homeland Security Bureau
PTIG	Project 25 Technology Interest Group
RAN	Radio Access Network
RECCWG	Regional Emergency Communications Coordination Working Group
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposals
RM	Resource Messaging
RUS	Rural Utilities Service
SAA	State Administrative Agency
SAME	Specific Area Message Encoding
SCIP	Statewide Communication Interoperability Plan
SDO	Standard Development Organization
SIGB	Statewide Interoperability Governing Body
SIEC	Statewide Interoperability Executive Committee
SLIGP	State and Local Implementation Grant Program
SOP	Standard Operating Procedure
SoR	Statement of Requirements
SPOC	Single Point of Contact
SPR	State Preparedness Report
SWIC	Statewide Interoperability Coordinator
TDoS	Telephone Denial of Service
TFOPA	Task Force on Optimal Public Safety Answering Point Architecture
THIRA	Threat and Hazard Identification and Risk Assessment
TIA	Telecommunications Industry Association
TICP	Tactical Interoperable Communications Plan
TSP	Telecommunications Service Priority
UASI	Urban Areas Security Initiative
UHF	Ultra High Frequency

Appendix A—Acronym List

USDA	United States Department of Agriculture
URT	Unified Reporting Tool
US-CERT	U.S. Computer Emergency Readiness Team
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
W3C	World Wide Web Consortium
WEA	Weather Emergency Alerts
WPS	Wireless Priority Service
XML	Extensible Markup Language

Appendix B – Technology and Equipment Standards

Grantees should purchase standards-based and advanced technologies that promote interoperability. When procuring equipment for communications systems, whether voice or data, an open standards-based approach should be used to facilitate interoperability between jurisdictions and disciplines at all levels of government, and to ensure interoperability between Federally-funded investments. This appendix provides the applicable requirements and resources for the following emergency communications capabilities:

- Land Mobile Radio (LMR)
  - TIA-102 Suite of Standards for Project 25 (P25)
  - P25 Resources
  - Standards for Voice over Internet Protocol (VoIP)
- Next Generation 911 (NG911)
  - Standards for NG911
  - NG911 Resources
- Public Safety Broadband
  - Nationwide Public Safety Broadband Network (NPSBN)
  - Standards for Other Broadband Technologies
  - Public Safety Broadband Resources
- Data Information Sharing Systems
  - Organization for the Advancements of Structured Information Standards (OASIS) Emergency Data eXchange Language (EDXL)
  - National Information Exchange Model (NIEM)
- Alerts and Warnings
  - Standards for Integrated Public Alert and Warning System (IPAWS)
  - Alerts and Warnings Resources
- Cybersecurity for Emergency Communications
  - Cybersecurity Best Practices
  - Standards for Cybersecurity
  - Cybersecurity Resources

Land Mobile Radio

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 critical requirements and support time-sensitive, lifesaving tasks, including rapid voice call-setup, group calling capabilities, high-quality audio, and priority access to the end-user. Because LMR systems 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 network infrastructure use and development. LMR systems will remain the primary tool for mission critical voice communications for many years to come; in fact, for many public safety agencies, maintaining their LMR systems and improving operability and interoperability continue to be their top communications priorities.

To maximize opportunities to improve interoperability across investments, grantees should ensure that digital voice systems and equipment purchased with Federal grant funds are compliant with the P25 suite of standards, unless otherwise noted in a program's grant guidance.[68] The P25 suite of standards is published by the Telecommunications Industry Association (TIA),[69] a recognized American National Standards Institute (ANSI) standards development organization. P25 standards provide a number of technical specifications for emergency communications equipment that are designed to ensure that equipment is interoperable regardless of manufacturer.

The P25 Steering Committee, in coordination with the P25 User Needs Subcommittee, publishes the P25 Users Statement of Requirements (SoR) that addresses user needs on an annual basis. Although the SoR reflects the user needs for LMR specifications and standards, it is not a part of the TIA-P25 standards and may contain requirements that are not addressed in the standards and are not available in existing products. It should be noted that the SoR should not be a replacement for detailed engineering specifications provided by the granting agency.

Standards for P25

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. The test documents include performance, conformance, and interoperability test procedures to ensure baseline compliance with the applicable standards. To ensure equipment and systems are compliant with the P25 suite of standards, grantees should:

- Review the technical specifications detailed in the P25 Technology Interest Group's (PTIG) *Capabilities Guide*[70] to determine which standards are applicable to the proposed purchase and project.
- Include all applicable P25 standards and expectations for interoperability in any SoR or bid for communications procurements funded through Federal grants.
- 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, grantees must ensure the standards-based feature or capability is included as well.

---

[68] Grantees should read grant guidance carefully to ensure compliance with standards, allowable cost, documentation, reporting, and audit requirements.

[69] The published standards approved by the P25 Steering Committee are available to employees of government agencies at no cost by completing the TIA on-line request form for government agencies at: http://www.tiaonline.org/all-standards/p25-downloads-application.

[70] The PTIG *Capabilities Guide* can be found on the PTIG website. To register visit: http://www.project25.org/.

- 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 Program's (CAP) Compliance Assessment Bulletins for testing requirements. When purchasing P25 LMR equipment and systems, grantees should, at a minimum, ensure the vendor has participated in equipment testing consistent with the P25 CAP.[71] If documentation for applicable equipment is not available through the P25 CAP, grantees 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.

Securing documentation of compliance through the P25 CAP is strongly recommended. However, information provided through the manufacturer will be beneficial to verify that equipment purchased is P25-compliant and is interoperable with other P25 systems and equipment when the applicable P25 feature, function, or interface is used in accordance with the standard.

If encryption is required, agencies shall ensure compliance with the P25 standard for the Advanced Encryption Standard (AES), when applicable. To ensure interoperability of encrypted communications between response agencies, devices used by responders must share a common encryption key and algorithm. The following provides additional guidance on encryption:

- Grantees using Federal funds to purchase encryption options for new or existing communications equipment should ensure that encrypted capabilities are compliant with the published P25 Block Encryption Protocol Standard. Grantees investing in encryption are strongly encouraged to implement the 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.
- Grantees seeking to use Federal grant funds to purchase non-standard encryption features or capabilities for new or existing equipment must ensure 256-bit AES is also included to ensure their devices have the capability to interoperate in an encrypted mode.
- Grantees 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.

[71] Equipment covered in the *P25 Compliance Assessment Program Requirements* document is tested in accordance with applicable standards and policies of the P25 CAP, and evidence of this testing is documented through Supplier's Declarations of Compliance and Summary Test Reports.

In the event a grantee is using Federal funds to purchase equipment that does not align with P25 standards, written justification should be provided to the grantor. Authorizing language for most emergency communications grants strongly encourages investment in standards-based equipment. Many agencies will not approve non-standards-based equipment unless there are compelling reasons for using other solutions. 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 compelling reason 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.

P25 Resources

Grantees should be aware that a wide range of LMR information is available from government and industry resources, including:

- PTIG: http://www.project25.org/ (Free registration required)
- P25 Suite of Standards: http://www.tiaonline.org/all-standards/committees/tr-8
- P25 Suite of Standards for Government Entities: http://www.tiaonline.org/all-standards/p25-downloads-application
- P25 CAP Information: http://www.firstresponder.gov/Pages/P25CAP.aspx?s=Saver

Standards for LMR and VoIP Systems Interfaces

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.

Next Generation 911 (NG911)

Next Generation 911 is an Internet Protocol (IP)-based system that allows digital information (e.g., voice, photos, videos, text messages) to flow seamlessly from the public through the 911 network and on to emergency responders. NG911 also enables new functions, such as the transfer and rerouting of 911 calls and data from one Public Safety Answering Point (PSAP) to another. While the technology to implement NG911 systems is available now, the transition to NG911 involves considerable planning and coordination. Implementing NG911 requires coordination with numerous stakeholders, who will plan and deploy a continually evolving system of hardware, software, standards, policies, protocols, and training.

Standards for NG911

A variety of technical and operational standards for the implementation of NG911 already exist, and many are actively under development. The National 911 Program maintains the *NG911*

Standards Identification and Review, a comprehensive listing of existing and planned standards for NG911 systems. This compilation of NG911 standards has been reviewed by the government and industry Standards Development Organizations (SDOs) whose standards are included in the document and the status of specific standards is updated annually. As NG911 standards continue to evolve, grantees should consult the *NG911 Standards Identification and Review* to ensure that solutions developed or procured meet industry guidelines and standards. Grantees and the 911 community are encouraged to consider the following options[72] when planning and implementing NG911:

- Strive for IP-enabled 911 open standards and understand future technology trends to encourage system interoperability and emergency data sharing[73]
- Establish routing and prioritization and business rules
- Determine the responsible entity and mechanisms for location acquisition and determination
- Establish system access, security controls, and comprehensive cybersecurity plans to protect and manage access to the IP-enabled 911 system of systems
- Develop a certification and authentication process to ensure service providers and 911 authorities meet security and system access requirements
- Establish collaborative relationships and mechanisms that facilitate the ongoing coordination required to plan, deploy, operate, and maintain NG911 systems
- Develop contract language that ensures the accountability of contractors in building, testing, deploying, operating, and maintaining interoperable and secure NG911 systems

NG911 Resources

The National 911 Program maintains a website from which grantees can access general information, standards, and State and local points of contact. Grantees may also access the 911 Resource Center, a clearinghouse for 911 authorities and professionals, and national 911 profile database. Key resources include:

- National 911 Program website: http://www.911.gov/
- *NG911 Standards Identification and Review*: http://www.911.gov/standardsfornextgen.html
- *Benefits of NG911*: *A Video:* http://www.911.gov/ng911movie.html
- *"State of 911" Webinars*: http://www.911.gov/webinars.html
- *NG911 for Leaders in Law Enforcement*: http://www.911.gov/ng911_law/download/ng911_resize_mar2013_final_lr.pdf

National Association of State 911 Administrators

The National Association of State 911 Administrators (NASNA) facilitates coordination and information sharing between State programs that administer 911 systems. Additional

[72] The National 911 Program identified these options in the *National Plan for Migration to IP-enabled Systems*. Available at: http://www.911.gov/pdf/National_NG911_Migration_Plan_FINAL.pdf.

[73] Standards addressing data format and system interfaces are particularly important to enable an emergency communications system that seamlessly transfers digital data from the caller to 911, and on to emergency responders.

information about the organization, along with their member organizations is available at their website: http://www.nasna911.org.

National Emergency Number Association

The National Emergency Number Association (NENA) serves the public safety community focusing on 911 policy, technology, operations, and education issues. NENA works with public policy leaders; emergency services and telecommunications industry partners; like-minded public safety associations; and other stakeholder groups to develop and carry out critical programs and initiatives; to facilitate the creation of an IP-based NG911 system; and to establish industry leading standards, training, and certifications. More information about NENA's NG911 efforts is available at: http://www.nena.org/?NG911_Project.

Association of Public Safety Communications Officials

The mission of the Association of Public-Safety Communication Officials (APCO) is to provide complete public safety communications expertise, professional development, technical assistance, advocacy, and outreach to benefit members and the public. In addition to these activities, APCO is also an ANSI-accredited standards developer. More information on APCO standards can be found at: https://www.apcointl.org/standards.html.

Federal Communications Commission (FCC)

The FCC's Public Safety & Homeland Security Bureau (PSHSB) is responsible for developing, recommending, and administering the agency's policies pertaining to 911, Enhanced 911 (E911), and NG911 services, including E911 location accuracy, 911 reliability, text-to-911, and the migration to NG911. More information is available at: https://www.fcc.gov/general/9-1-1-and-e9-1-1-services. In addition, the FCC's Task Force on Optimal Public Safety Answering Points (PSAP) Architecture (TFOPA), a federal advisory committee, is developing reports and recommendations regarding actions that PSAPs can take to optimize their security, network architecture, and funding as they migrate to NG911 Information on TFOPA is available at: https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point. Finally, the FCC's Communications Security Reliability and Interoperability Council (CSRIC) provides advice and recommendations to the FCC from a formal advisory body. Information on the fifth iteration of CSRIC is available at: https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-v.

Public Safety Broadband

Nationwide Public Safety Broadband Network

The First Responder Network Authority's (FirstNet) mission is to ensure the building, deployment, operation, and maintenance of the NPSBN that will use the 700 MHz public safety

spectrum[74] to provide broadband services and applications to the public safety community. The network will be based on, but may exceed, the minimum technical requirements for commercial Long-Term Evolution (LTE) service. Congress required that the NPSBN be based on a single, national network architecture consisting of a core network, transport backhaul, radio access network (RAN). While mission critical voice communications will continue to occur exclusively on LMR, the NPSBN is expected to provide the public safety community with the following capabilities:

- Messaging
- Image Sharing
- Video Streaming
- Group Text
- Non-Mission Critical Voice
- Data Storage
- Applications

FirstNet is still developing the network architecture, technical and user requirements, spectrum access policies, standards, and deployment plans. FirstNet continues to actively engage public safety entities, Federal, state, local, tribal, and territory jurisdictions, and other stakeholders to plan for the network. To assist states and territories in preparing for the NPSBN, the National Telecommunications and Information Administration (NTIA), in consultation with FirstNet, awarded $116.5 million in grants to 54 U.S. states and territories through the State and Local Implementation Grant Program (SLIGP). This funding provides recipients with the resources to work with stakeholders throughout the state or territory to identify needs, gaps, and priorities for public safety wireless broadband and to prepare for consultation with FirstNet.

While entities may want to pursue funding for broadband equipment and systems on the designated spectrum, there are no assurances that such equipment and systems will be compatible with and capable of NPSBN integration.[75] Therefore, FirstNet strongly advises grantees to avoid strategic acquisition of LTE equipment until there is further guidance from FirstNet on technical requirements and network deployment. Grantees are encouraged to focus funding on planning and outreach activities (e.g., community outreach and education, documenting user needs) and to work with the Single Point of Contact (SPOC) [76] in planning for the arrival of broadband and other advanced technologies.[77] This includes:

---

[74] The Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96) authorized the establishment of the NPSBN, dedicated broadband spectrum for its users, and named FirstNet as the single licensee for the combined 700 MHz public safety and D Block spectrum. The public safety broadband spectrum band is 763-768 MHz and 793-798 MHz.

[75] There are certain entities that have approval from FirstNet to proceed with broadband acquisition and deployment through a spectrum management lease agreement. These entities have been granted spectrum access and permission to proceed with planned broadband projects funded under the Broadband Technology Opportunities Program (BTOP) and the Department of Homeland Security (DHS), which were awarded prior to passage of the Middle Class Tax Relief and Job Creation Act of 2012. For more information on these projects, please contact OEC at oec@hq.dhs.gov.

[76] Appointed by the governor of each State and territory, an individual or body serves as the Single Point of Contact (SPOC) to engage in consultation with FirstNet for the planning of the NPSBN. The SPOC is responsible for implementing the SLIGP grant and engaging in consultation with FirstNet to help with the design and implementation of the NPSBN. The SPOC contact list is available at: http://firstnet.gov/consultation.

[77] The term "advanced technologies" includes, but is not limited to, the use of emerging technologies to provide advanced interoperability solutions; solutions that allow the use of commercial services, where appropriate, to support interoperable communications; IP-based technologies; use of common advanced encryption options that allow for secure and vital

- Attending statewide or regional broadband planning meetings
- Establishing a governance structure, or expanding existing structures, to consult with FirstNet
- Preparing a comprehensive plan as part of the existing Statewide Communication Interoperability Plan (SCIP), or a plan complementary to and similar in concept to the SCIP, describing the public safety needs that the State or territory expects FirstNet to address in its design of the NPSBN
- Developing procedures to ensure regional, local, and tribal representation and participation in the consultation process with FirstNet
- Ensuring that all necessary planning and tribal consultation for Federal environmental, historic preservation and cultural resources statutory compliance will occur
- Creating and implementing a process for education and outreach, through program development or through other efforts, among regional, local, and tribal officials, public safety users, and other stakeholders about the NPSBN
- Identifying potential public safety users of the NPSBN
- Developing staffing plans that include regional, local, and tribal representation to participate in the public safety governance structure and to prepare for data collection activities in consultation with FirstNet
- Planning for integration of IT infrastructure, software, and site upgrades necessary to connect to the NPSBN

Grantees 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. Grantees should also consult with their SPOC and FirstNet during the development of the application to ensure the project does not conflict with NPSBN planning efforts and comply with any technical requirements. Grantees should continue to monitor current Federal actions affecting broadband investments.

Standards for Other Wireless Broadband Technologies

Over the past several years, public safety agencies have leveraged non-LTE wireless broadband technologies (e.g., Wi-Fi, WiMAX, mesh networks) to supplement current 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. The use of common standards-based commercial technologies (i.e., IEEE 802.11n) minimizes interoperability concerns among vendors of a given technology, and the sharing of wireless network infrastructures may reduce immediate costs for State and local public safety systems.[78]

However, given ongoing advancements in the NPSBN deployment and interoperability challenges of various technologies, grantees should consider the overall impact of using other wireless broadband technologies at this time. Before the Middle Class Tax Relief and Job Creation Act established minimum technical requirements for the NPSBN to be based upon LTE,

transmissions, while maintaining interoperability; use of standards-based technologies to provide voice and data services that meet wireless public safety service quality; solutions that have an open interface to enable the efficient transfer of voice, data, and video signals; and investments in these technologies, such as NG911 and Bridging System Interface.

[78] FCC Tech Topic #11: WiMAX Applications for Public Safety at: http://transition.fcc.gov/pshs/techtopics/techtopics11.html.

public safety agencies considered other wireless broadband technologies such as WiMAX. LTE was endorsed by public safety organizations for economies of scale, radio frequency use, and spectral efficiency reasons.[79] Moreover, major wireless service providers chose LTE for their broadband data services and in 2010, the FCC designated LTE as the required technology for the NPSBN.[80] Thus, grantees are strongly encouraged to focus on preparation for the NPSBN and working with FirstNet and their SPOC to assess broadband user needs.

With these cautions, grantees 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. Grantees 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. Grantees are encouraged to implement innovative solutions that will yield improvements to current communications capabilities and help the agencies plan for and prepare for the deployment of the NPSBN.

Public Safety Broadband Resources

700 MHz Public Safety Broadband Network

- FirstNet: http://www.firstnet.gov/
- NTIA public safety website: http://www.ntia.doc.gov/category/public-safety
- FCC website: http://www.fcc.gov/encyclopedia/700-mhz-spectrum
- Public Safety Communications Evolution Brochure: http://www.dhs.gov/safecom/resourceslibrary
- Public Safety Communications Research (PSCR) Demonstration Network: http://www.pscr.gov/projects/broadband/700mhz_demo_net/700mhz_ps_demo_net.php

Broadband

- Standards for Other Broadband Technologies: FCC Tech Topic #11: WiMAX Applications for Public Safety at: http://transition.fcc.gov/pshs/techtopics/techtopics11.html
- Application of Emerging Wireless Broadband Technology for Public Safety Communications: FCC Tech Topic #22: http://transition.fcc.gov/pshs/techtopics/techtopics22.html

Existing Programs

- Broadband Technology Opportunities Program: http://www2.ntia.doc.gov/
- Broadband Initiatives Program: http://www.rurdev.usda.gov/utp_bip.html
- USDA Rural Utilities Farm Bill Broadband Loan Program: http://www.rurdev.usda.gov/RUSTelecomPrograms.html

FirstNet

- http://firstnet.gov/

[79] See: http://www.npstc.org/documents/Press_Release_NPSTC_Endorses_LTE_Standard_090610.pdf.
[80] FCC, 700 MHz Public Safety Spectrum: http://www.fcc.gov/encyclopedia/700-mhz-spectrum.

Interoperability Planning for Wireless Broadband

- http://www.dhs.gov/safecom/resourceslibrary

Middle Class Tax Relief and Job Creation Act

- To obtain a copy of the Act, see: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3630enr/pdf/BILLS-112hr3630enr.pdf
- Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation: http://www.dhs.gov/public-safety-broadband-fulfilling-911-commission-recommendation

National Broadband Plan

- http://www.broadband.gov/plan/

Public Safety Communications Research (PSCR) Demonstration Network

- http://www.pscr.gov/projects/broadband/700mhz_demo_net/700mhz_ps_demo_net.php

State and Local Implementation Grant Program (SLIGP)

- http://www.ntia.doc.gov/category/state-and-local-implementation-grant-program

Data Information Sharing Systems

Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data eXchange Language (EDXL)

The 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 OASIS EDXL suite of data messaging standards. Compliance should include the following OASIS EDXL standards:

- Common Alerting Protocol (CAP), version 1.1 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

This guidance does not preclude funding of non-OASIS EDXL compliant systems when there are compelling reasons for using other solutions. In the case that the system does not comply with OASIS EDXL, it should still conform to the National Information Exchange Model. Funding requests by agencies to use non-OASIS EDXL compliant systems will be considered if there is a compelling reason why such equipment should be purchased, and written justification of how the equipment will advance interoperability and how the purchase will support eventual migration to interoperable systems. Absent such compelling reasons, the OASIS EDXL standards are the preferred standards. For more information, see: http://www.oasis-open.org.

National Information Exchange Model (NIEM)

NIEM is a framework established by the Department of Homeland Security (DHS) and the Department of Justice to enable streamlined and secure information sharing of data among

Federal, State, local, tribal, and territorial agencies, and with private sector entities. NIEM focuses on cross-domain information exchange across multiple levels of government, thereby allowing organizations and agencies to share information quickly and effectively without rebuilding systems. Federally-funded systems supporting emergency response information sharing should refer to the NIEM conformance rules to implement their information sharing exchanges.

NIEM is not a software program, a computer system, or a data repository but a framework made up of two key components:

- A data dictionary of more than 7,000 terms that are commonly used in an information exchange
- A repeatable, reusable process for developing information exchange requirements

In NIEM, a "data exchange" is also known as the Information Exchange Package (IEP), a description of specific information exchanged between a sender and a receiver. The IEP is usually coupled with additional documentation, sample Extensible Markup Language (XML) instances, business rules, and more to compose an Information Exchange Package Documentation (IEPD). The resulting work product is an IEPD, which is a set of artifacts that define a particular data exchange. NIEM provides rules and guidance regarding the content of artifacts in an IEPD and the format of those artifacts in order to promote consistency. For example, there is an IEPD that defines the information content and structure for an AMBER Alert, a bulletin or message sent by law enforcement agencies to announce the suspected abduction of a child. IEPDs define the process by which data is exchanged and is currently used by all 50 States.[81]

Alerts and Warnings

During an emergency, alert and warning systems enable public safety officials to provide the public with information quickly. The Integrated Public Alert and Warning System (IPAWS) is a modernization and integration of the Nation's alert and warning infrastructure, administered by the Federal Emergency Management Agency (FEMA). Federal, State, local, tribal, and territorial alerting authorities can use IPAWS and integrate local systems that use the Common Alerting Protocol (CAP) standard with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, the IPAWS All-Hazards Information Feed, and other public alerting systems from a single interface.

[81] Grantees are encouraged to reference the NIEM website to develop a greater understanding of data exchange functions and processes. Information on NIEM can be found at: https://www.niem.gov/Pages/default.aspx. In addition, NIEM has developed specific guidance for grantees which can be found at: https://www.niem.gov/aboutniem/grant-funding/Pages/implementation-guide.aspx.

Standards for IPAWS

In order to access IPAWS, grantees should select equipment and applications that adhere to both CAP and the IPAWS Profile standards. The CAP standard is an open, non-proprietary digital format for exchanging emergency alerts that was developed by 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 that include images, maps, and video.

In addition to CAP, 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 the supplemental IPAWS Profile ensure compatibility with existing warning systems used throughout the country.

Alert and warning software and equipment is developed, produced, and distributed by various vendors. The IPAWS Program Management Office (PMO) does not endorse any specific vendor or any specific piece of software or equipment. Test results for any alert and warning software or equipment tested at the IPAWS laboratories can be made available to assist grantees in making procurement decisions by contacting the IPAWS PMO at ipaws@dhs.fema.gov.

Grantees should select software or equipment that also supports regional operable and interoperable solutions. Grantees 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. Alert and warning grant funds should focus on eligible public alert and warning activities to include, but not limited to the purchase, training, replacement, and maintenance of alert and warning systems, software, and equipment.

Alerts and Warning Resources

CAP and IPAWS Profile

- https://www.fema.gov/common-alerting-protocol

IPAWS

- IPAWS Program Office: https://www.fema.gov/integrated-public-alert-warning-system
- Informational Materials: https://www.fema.gov/informational-materials
- State and Local Alerting System Authorities: https://www.fema.gov/integrated-public-alert-warning-system-authorities

OASIS

- https://www.oasis-open.org/

Cybersecurity for Emergency Communications

The emergency response community is deploying advanced voice, video, and data services over 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.

Despite the extent of critical infrastructure protection, it will be attacked or face vulnerabilities in hardware, software, or policy. The U.S. Computer Emergency Readiness Team (US-CERT) reported 48,842 incidents in 2012 on Federal Government systems and 104,201 incidents on State, local, tribal, and territorial governments, and commercial entities. For example, attackers have disrupted availability of traditional 911 systems by using auto-dialers to overwhelm PSAP phone lines and cause congestion, preventing legitimate 911 calls from going through [commonly called Telephone Denial of Service (TDoS) attacks]. As cyber threats grow in complexity and sophistication, attacks could become more numerous and severe against an emergency communications system. Recipients should be aware of the type of associated risks with these technologies. Table B-1 identifies potential cyber risks to various components of emergency communications systems.

Table B-1. Cyber Risks to Emergency Communications Systems

Components	Cyber Risks
Devices and Equipment	• Data breaches: Data stored on user is accessed, manipulated, or stolen • Malware: Users download malicious software (e.g., botnets, viruses, spyware, Trojans, rootkits) • Spear-phishing: Targeted social engineering attacks aimed at system users that enable hackers to access sensitive data
Network Infrastructure and Connections	• Man-in-the-middle attacks: Wireless link between the user device and the tower may be susceptible and allow attackers to steal data or monitor conversations • Denial-of-service attacks: Attackers overload the network resources with requests for network access, impeding the operability of the network • Unauthorized network access: Attackers gain network access using stolen credentials and/or devices
Data, Applications, and Services	• Insider threats: Employees or other authorized personnel use their access to steal, corrupt, or destroy data • Malicious applications: Attackers create applications that appear to be safe but allow them to steal, corrupt, or modify data, eavesdrop on conversations, or acquire data on the location of emergency responders • Unauthorized data access: Attackers can access sensitive databases (e.g., law enforcement, health records) to steal, modify, or corrupt data

To protect emergency communications networks from cyber threats and attacks, recipients will need to invest in cybersecurity[82] solutions. Cybersecurity efforts should include planning and governance, in addition to technical solutions that identify, mitigate and secure networks, to ensure compliance with applicable cyber standards and requirements. Recipients should ensure that 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.

[82] DHS *National Infrastructure Protection Plan* defines cybersecurity as "the prevention of damage to, unauthorized use of, or exploitation of, and if needed, the restoration of electronic information and communications systems and the information contained."

Cybersecurity Best Practices

Recipients should invest in the adoption of cybersecurity best practices that address threats and risks posed by their individually unique user requirements, operational needs, and system and infrastructure. Recipients should also consider establishing a Computer Security Incident Response Team (CSIRT) or reach an agreement with US-CERT to assist in carrying out cybersecurity planning. US-CERT is a CSIRT run by DHS's National Cybersecurity and Communications Integration Center (NCCIC). A CSIRT serves as a centralized location to report and analyze security issues within an organization. A CSIRT may also recommend potential solutions to the threats and publicize known threats, vulnerabilities, and solutions generally or to a specific information-sharing community. The CSIRT could also work with hardware and software vendors to obtain information about vulnerabilities and potential solutions.

The first step in developing a comprehensive cybersecurity plan is investing in the development, adoption, and continuous update of a cybersecurity management framework. The National Institute of Standards and Technology (NIST) developed the *Framework for Improving Critical Infrastructure Cybersecurity* as a flexible and voluntary risk-based approach that outlines techniques to secure critical infrastructure.[83] Recipients are strongly encouraged to adopt 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 NIST Cybersecurity Framework.[84] Organizations seeking to improve their cybersecurity posture are strongly encouraged to access the Framework to help manage cybersecurity risks.

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. Table B-2 highlights some fundamental cybersecurity best practices for recipients to reference in the development of a more tailored and comprehensive cybersecurity strategy.

[83] For more information on the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, see: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[84] Critical Infrastructure Cyber Community C³ Voluntary Program, http://www.dhs.gov/ccubedvp.

Table B-2. Cybersecurity Best Practices

Functions	Best Practices
Identify	Identify Threats • Identify all system assets • Examine historical data for past accidents and attacks • Review notifications from government cybersecurity resources, hardware and software vendors, and academic sources on potential vulnerabilities. • Receive threat information directly from sources (e.g., US-CERT) Identify Vulnerabilities • Review procedures for gaps in patching and managing updates • Review identity management practices and internal controls to prevent accidents • Review available government, industry and academic cybersecurity resources for gaps against cybersecurity posture and standards • Identify impact to confidentiality, integrity, and availability of system and data if a threat exploits a vulnerability Evaluate • Examine likelihood, intent, and resources necessary for a threat to exploit a vulnerability • Examine consequences of threat and how an attack may impact overall operations Prioritize Risk • Plot risks on a risk map using the likelihood and consequences ratings • Prioritize risks based on the risk map and stakeholder feedback • Use risk prioritization to make informed decisions regarding risk mitigation investment
Protect	• Access Privileges. Ensure appropriate use and accurate assignment of privileges amongst personnel • Authentication and Identity Management. Develop, implement, and apply uniform authentication and identity management policies that meet public safety requirements for performance and time-sensitive demands • Capacity Planning. Engage in assessing capacity requirements for infrastructure and assets • Data Encryption. Develop requirements for data encryption that apply to both primary and backup data • Security Policies. Establish, enforce, and update consistent information security policies as new threats emerge • Training. Develop role-specific training for users and administrators on security, resiliency, and operations
Detect	• Continuous Monitoring. Develop or use existing government continuous monitoring diagnostics and mitigation capabilities, such as DHS' Continuous Diagnostics and Mitigation (CDM) Program[85] • Log Management and Audit Capabilities. Ensure log management policies and audit capabilities are strong, appropriate, and responsive • Physical Security and Access Control. Develop and implement physical security and access control policies
Response	• Incident Response Plan. Develop incident response plans, policies, and capabilities for the networks, personnel and user equipment that prevent expansion of the event, mitigate its effects, and eradicate the incident • Incident Response Team. Establish an incident response team with or utilize existing capabilities like US-CERT to ensure response activities are coordinated with appropriate stakeholders
Recovery	• Recovery Plan. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event • Continuity Planning. Establishing and maintaining redundancy is a key strategy that promotes network reliability, resiliency, and continuity of service • Coordination. Restoration activities are coordinated with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, response partners, and vendors • Process Improvements. Recovery planning processes and strategies are improved by incorporating lessons learned into future activities. Response 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

[85] DHS CDM Program, http://www.dhs.gov/cdm.

Standards for Cybersecurity

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-3 lists the applicable standards for cybersecurity that recipients should leverage as they identify and select the standards that fit their system and mission needs. While the list below is not exhaustive, it does include some of the more comprehensive guidance for the emergency community.

Table B-3. Cybersecurity Standards

Standard	Intent
ANSI/ISA[86]	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.
Criminal Justice Information Services (CJIS) Security Policy[87]	CJIS standards contain information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI).
European Telecommunications Standards Institute (ETSI)[88]	ETSI Telecommunications & Internet converged Services & Protocols for Advanced Networks (TISPAN) has been a key standardization body in creating NGN specifications, and their Cyber Security committee (TC CYBER) focuses entirely on privacy and security activities. Of note for emergency communications are the ETSI TS 102, 123, 182, and 282 series.
Federal Information Processing Standards (FIPS)	Establishes the minimum security requirements for Federal information and information systems.
IEEE[89]	IEEE produces sector-specific security standards, as well as industry guidance. Of particular interest 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.
International Organization for Standardization (ISO) /International Electrotechnical Commission (IEC) Standards[90]	The ISO/IEC 27000 series of standards provide a foundation for information security management best practices. Specifically of interest to emergency communication networks may be ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27002, ISO/IEC 27032, and ISO/IEC 17799.
International Telecommunications Union (ITU)	A fundamental role of ITU is to build confidence and security in the use of Information and Communication Technologies (ICT). Of note for emergency communications include X.800, X.805, and X.1051.
Internet Engineering Task Force (IETF)[91]	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.
NENA Security for NG911 Standard (NG-SEC).	NENA 75-001: NENA Security for Next Generation 911 Standard (NG-SEC) NENA 75-502: NG-SEC Audit Checklist NENA 04-503: Network/System Access Security Information Document

[86] ANSI/ISA standards, https://www.isa.org/templates/two-column.aspx?pageid=131422.
[87] CJIS Security Policy, https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.
[88] ETSI, http://www.etsi.org/.
[89] IEEE, http://www.ieee.org/.
[90] ISO, http://www.iso.org.
[91] IETF, https://www.ietf.org/.

Standard	Intent
National Fire Protection Association 1221[92]	A standard for the installation, maintenance, and use of emergency services communications systems, and includes cybersecurity considerations.
Next Generation 911 (NG911) Program Standards Identification and Review[93]	These standards collected from all major standards bodies and address cybersecurity when planning for NG911 deployments.
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.
North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Regulations[94]	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.
Organization for the Advancement of Structured Information Standards (OASIS)[95]	OASIS Emergency Management Technical Committee (EM-TC) creates incident- and emergency-related standards for data interoperability: Common Alerting Protocol (CAP); 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).
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.
Third Generation Partnership Project (3GPP) Security Standards[96]	3GPP's security working group, SA3, is continuously updating security standards associated with prevalent technologies, most notably LTE and IP Multimedia Subsystem (IMS). 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.
World Wide Web Consortium (W3C)[97]	Includes web cryptography, web application security, web payments, and XML security.

Cybersecurity Resources

Recipients should be aware of other resources that help establish or update the methods, techniques, policies, and/or procedures necessary to improve cybersecurity. Below are applicable government directives, templates, and other information sources to assist in cybersecurity risk management.

Committee on National Security Systems (CNSS) Guidance

- Policies: https://www.cnss.gov/CNSS/issuances/Policies.cfm

DHS

- Communications Sector-Specific Plan (CSSP): An Annex to the National Infrastructure Protection Plan: https://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf

[92] National Fire Protection Association 1221, http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1221.
[93] NG911 Program Standards Identification and Review, http://www.911.gov/pdf/NG911-StandardsIdentificationAnalysis-jan2014.pdf.
[94] NERC Critical Infrastructure Protection Regulations, http://www.nerc.com/pa/CI/Comp/Pages/default.aspx
[95] OASIS, https://www.oasis-open.org/.
[96] 3GPP, www.3gpp.org.
[97] W3C, https://www.w3.org/.

- Continuous Diagnostics and Mitigation (CDM): http://www.gsa.gov/portal/content/177895
- Emergency Services Sector (ESS) Cyber Risk Assessment – 2012: http://www.dhs.gov/publication/emergency-services-sector-cybersecurity-initiative
- Homeland Security Grant Program Supplemental Resource: Cyber Security Guidance: http://www.fema.gov/media-library-data/1395241351544-a69a6ae018646cd2bb8f61a6a0e2bee3/FY%202014%20Supplemental%20Guidance_Cybersecurity.pdf
- Intrusion Detection (IDS) and Intrusion Prevention (IPS): http://www.dhs.gov/cybersecurity-and-privacy
- National Cybersecurity and Communications Integration Center (NCCIC) and US-CERT: http://www.dhs.gov/national-cybersecurity-communications-integration-center
- National Infrastructure Coordinating Center (NICC): http://www.dhs.gov/national-infrastructure-coordinating-center
- National Infrastructure Protection Plan (NIPP): http://www.dhs.gov/national-infrastructure-protection-plan
- Network Flow Collection: https://msisac.cisecurity.org/about/services
- Safeguarding and Securing Cyberspace: https://www.dhs.gov/xlibrary/assets/pso-safeguarding-and-securing-cyberspace.pdf
- Supplement Tool: Executing a Critical Infrastructure Risk Management Approach: http://www.dhs.gov/publication/executing-critical-infrastructure-risk-management-approach
- Supplement Tool: NPPD Resources to Support Vulnerability Assessments: http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_NPPD%20Resources%20to%20Support%20VAs_508.pdf
- Trusted Internet Connections: http://www.dhs.gov/trusted-internet-connections

Executive Orders (EO) and President Directives

- EO 13636: Improving Critical Infrastructure Cybersecurity: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- EO 13231: Critical Infrastructure Protection in the Information Age and EO 13286: http://www.fas.org/irp/offdocs/eo/eo-13231.htm
- EO 13618: Assignment of National Security and Emergency Preparedness Communications Functions: https://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-
- Executive Office of the President, Presidential Policy Directive 21 (PPD- 21): https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

FCC

- Communications Security, Reliability and Interoperability Council (CSRIC): https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability

NIST

- Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/
- Internal/Interagency Reports (NISTIR): http://csrc.nist.gov/publications/PubsNISTIRs.html

Industry and Associations

- ATIS Industry Best Practices: http://www.atis.org/bestpractices/Search.aspx
- International Telecommunications Union (ITU) Security Standards Roadmap: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/default.aspx
- SANS Institute 20 Critical Security Controls: https://www.sans.org/critical-security-controls

Appendix C – Emergency Communications Resources

This Appendix provides links to resources referenced in the *FY 2016 SAFECOM Guidance* and additional resources to help grantees develop emergency communications projects and complete Federal grant applications. Grantees are strongly encouraged to visit the SAFECOM website (http://www.dhs.gov/safecom) for additional resources.

800 MHz Rebanding
- FCC Website: http://transition.fcc.gov/pshs/public-safety-spectrum/800-MHz/
- 800 MHz Transition Administrator Website: http://www.800ta.org/
- Transition Administrator Contact: comments@800TA.org

Association of Public-Safety Communications Officials (APCO)
- Information on APCO standards: https://www.apcointl.org/standards.html

Authorized Equipment List (AEL)
- For a list of interoperable emergency communications equipment typically allowed under emergency communications grants, see FEMA's AEL at: http://www.fema.gov/authorized-equipment-list

Broadband
- Standards for Other Broadband Technologies: FCC Tech Topic #11: WiMAX Applications for Public Safety at: http://transition.fcc.gov/pshs/techtopics/techtopics11.html
- Application of Emerging Wireless Broadband Technology for Public Safety Communications: FCC Tech Topic #22: http://transition.fcc.gov/pshs/techtopics/techtopics22.html
- Broadband Technology Opportunities Program (BTOP): http://www2.ntia.doc.gov/
- Broadband Initiatives Program: http://www.rurdev.usda.gov/utp_bip.html
- USDA Rural Utilities Farm Bill Broadband Loan Program: http://www.rurdev.usda.gov/RUSTelecomPrograms.html
- Interoperability Planning for Wireless Broadband: http://www.dhs.gov/safecom/resourceslibrary

Common Alerting Protocol (CAP)
- https://www.fema.gov/common-alerting-protocol

Cost Sharing/Matching Resources
- See *SAFECOM Guidance*, Section 3.4 – Understand Federal Grant Requirements and Restrictions

Data Information Sharing Systems, Standards
- See Appendix B in the *SAFECOM Guidance*
- See OASIS at: http://www.oasis-open.org

Environmental Planning and Historic Preservation (EHP) Resources
- See *SAFECOM Guidance*, Section 4.5 - *Additional Requirements and Recommendations for Equipment Purchases*
- For questions on EHP for FEMA grants, contact: GPDEHPInfo@fema.gov

Equipment Standards
- For guidance on equipment and equipment standards, see: *SAFECOM Guidance,* Section 4.5 and Appendix B

Exercise Resources
- For guidance on exercises, see the *SAFECOM Guidance,* Section 4.4
- Communications-Specific Tabletop Exercise Methodology: http://www.dhs.gov/safecom/resourceslibrary
- Exercises conducted for FEMA grants must be NIMS compliant. More information is available at: http://www.fema.gov/national-incident-management-system
- NIMS National Standard Curriculum Training Development Guidance: http://www.fema.gov/national-incident-management-system/training

Federal Communications Commission (FCC) Resources
- Public Safety & Homeland Security Bureau: https://www.fcc.gov/public-safety-homeland-security-bureau
- For information on licensing fees, see the FCC Fee Filing Guide for the Wireless Telecommunications Bureau at: http://transition.fcc.gov/fees/appfees.html
- Communications Security Reliability and Interoperability Council (CSRIC): https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-v
- Task Force on Optimal Public Safety Answering Point (PSAP) Architecture (TFOPA): https://www.fcc.gov/encyclopedia/task-force-optimal-public-safety-answering-point-architecture-tfopa

Federal Emergency Management Agency (FEMA) Information Bulletins
- http://www.fema.gov/grants/grant-programs-directorate-information-bulletins

First Responder Network Authority (FirstNet)
- http://firstnet.gov/

Governance
- Governance Guide for State, Local, Tribal, and Territorial Emergency Communications Officials: http://www.dhs.gov/safecom/governance

Grants Listings
- For a list of grants funding emergency communications, see: http://www.dhs.gov/funding
- Grants.gov Website: http://www.grants.gov
- FEMA Grants Website: http://www.fema.gov/grants

Integrated Public Alert and Warning System (IPAWS)
- IPAWS Program Office: https://www.fema.gov/integrated-public-alert-warning-system

- Information Materials on IPAWS: https://www.fema.gov/informational-materials
- State and Local Users: https://www.fema.gov/integrated-public-alert-warning-system-authorities

Intergovernmental Review

- Executive Order 12372 requires applicants from State and local units of government or other organizations providing services within a State to submit a copy of the application to the State Single Point of Contact (SPOC), and if this program has been selected for review by the State. Applicants must contact their State's SPOC to determine if the program has been selected for State review. Note: This is a different contact than the SPOC responsible for engaging with FirstNet on public safety broadband network activities.
  - Executive Order 12372 can be referenced at: http://www.archives.gov/federal-register/codification/executive-order/12372.html
  - Names and addresses of the SPOCs are listed at: www.whitehouse.gov/omb/grants_spoc

Land Mobile Radio

- Land Mobil Radio (LMR) Trio – LMR 101, LMR for Decision Makers, and LMR for Project Managers: http://www.dhs.gov/safecom/funding

Law Enforcement Resources

- Law Enforcement Tech Guide for Communications Interoperability: http://ric-zai-inc.com/ric.php?page=detail&id=COPS-W0714
- Law Enforcement Tech Guide Resources for Technology Project Management: http://ric-zai-inc.com/ric.php?page=detail&id=COPS-CD040

Life Cycle Planning

- For guidance on emergency communications system life cycle planning, see: http://www.dhs.gov/safecom/resourceslibrary

Middle Class Tax Relief and Job Creation Act

- To obtain a copy of the Act, see: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3630enr/pdf/BILLS-112hr3630enr.pdf
- Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation: http://www.dhs.gov/public-safety-broadband-fulfilling-911-commission-recommendation

Narrowbanding

- See *SAFECOM Guidance*, Section 3.3
- FCC Narrowbanding Website: http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html

National Association of State 911 Administrators (NASNA)

- State 911 Program Information: http://www.nasna911.org

National Emergency Communications Plan (NECP)

- For the NECP, see: http://www.dhs.gov/necp

National Emergency Number Association (NENA)

- NENA Next Generation 911 efforts: http://www.nena.org/?NG911_Project

National Incident Management System (NIMS)
- NIMS Website: http://www.fema.gov/national-incident-management-system
- ICS Resource Center: http://training.fema.gov/EMIWeb/IS/ICSResource/index.htm

National Information Exchange Model (NIEM)
- https://www.niem.gov/Pages/default.aspx

National Interoperability Field Operations Guide (NIFOG)
- http://www.dhs.gov/national-interoperability-field-operations-guide

National Preparedness Goal
- http://www.fema.gov/national-preparedness-goal

National Preparedness System
- http://www.fema.gov/national-preparedness-system

Nationwide Public Safety Broadband Network (NPSBN)
- FirstNet Website: http://firstnet.gov
- NTIA Public Safety Website: http://www.ntia.doc.gov/category/public-safety

National Public Safety Telecommunications Council (NPSTC)
- http://www.npstc.org/

Next Generation 911 (NG911)
- National 911 Program Website: http://www.911.gov/
- NG911 Standards Identification and Review: http://www.911.gov/911-issues/standards.html
- Benefits of NG911: A Video: http://www.911.gov/ng911movie.html
- "State of 911" Webinars: http://www.911.gov/webinars.html
- NG911 for Leaders in Law Enforcement: http://www.911.gov/ng911_law/download/ng911_resize_mar2013_final_lr.pdf

OASIS Emergency Data eXchange Language, Standards for Data-Related Investments
- http://www.oasis-open.org

Office of Emergency Communications (OEC)
- OEC Website: http://www.dhs.gov/about-office-emergency-communications
- OEC Contact Information: oec@hq.dhs.gov
- OEC Guidance Documents: http://www.dhs.gov/safecom/resourceslibrary
- OEC Technical Assistance Catalog: http://www.publicsafetytools.info/start_index.php

Office of Management and Budget (OMB) Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards
- OMB Grants Management website: http://www.regulations.gov/#%21documentDetail;D=OMB_FRDOC_0001-0127

Presidential Policy Directive–8 (PPD–8)
- For more information on PPD–8, see: http://www.dhs.gov/presidential-policy-directive-8-national-preparedness and http://www.fema.gov/ppd8

Priority Service Programs
- http://www.dhs.gov/gets

Project 25 (P25), Standards for Land Mobile Radio (LMR) Investments
- P25 Suites of Standards: http://www.tiaonline.org/all-standards/committees/tr-8
- P25 Suite of Standards for Government Entities: http://www.tiaonline.org/all-standards/p25-downloads-application
- P25 Technology Interest Group (PTIG): http://www.project25.org/
- P25 Compliance Assessment Program (CAP): http://www.firstresponder.gov/Pages/P25CAP.aspx?s=Saver

Public Safety Communications Evolution Brochure
- http://www.dhs.gov/safecom/resourceslibrary

Public Safety Communications Research (PSCR) Demonstration Network
- http://www.pscr.gov/projects/broadband/700mhz_demo_net/700mhz_ps_demo_net.php

Regional Guidance
- *Regional Interoperability Communications Plan Template:* http://www.dhs.gov/safecom/resourceslibrary

SAFECOM Program
- http://www.dhs.gov/safecom/

State Administrative Agency (SAA)
- https://www.fema.gov/media-library/assets/documents/28689

State and Local Implementation Grant Program (SLIGP)
- http://www.ntia.doc.gov/category/state-and-local-implementation-grant-program

Statewide Interoperability Coordinator (SWIC)
- See *SAFECOM Guidance*, Sections 3.2 and 4.2
- *Establishing Governance to Achieve Statewide Communications Interoperability*: http://www.dhs.gov/safecom/resourceslibrary

Statewide Communication Interoperability Plan (SCIP)
- See *SAFECOM Guidance*, Sections 2.2 and 4.2
- For information on SCIPs, see the OEC website at: http://www.dhs.gov/statewide-communication-interoperability-plans
- To find your SCIP, please contact your SWIC or SCIP Point of Contact. If you do not know your SWIC or SCIP Point of Contact, please email OEC at: oec@hq.dhs.gov

T-Band

- For an overview of T-Band issues, see: http://www.npstc.org/TBand.jsp
- The Middle Class Tax Relief and Job Creation Act of 2012 requires that systems operating in the T-Band migrate within 11 years of enactment, by 2023. See: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3630enr/pdf/BILLS-112hr3630enr.pdf

Technical Assistance

- OEC: http://www.publicsafetytools.info/start_index.php

Threat and Hazard Identification and Risk Assessment (THIRA)

- http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf

Training Resources

- Approved Federal Sponsored Course Catalog: http://www.firstrespondertraining.gov
- National Preparedness Directorate Online Course Catalog: http://www.firstrespondertraining.gov
- FEMA Training Catalogs: https://www.firstrespondertraining.gov/content.do?page=training

Voice-over-Internet Protocol (VoIP) Standards

- http://www.pscr.gov/outreach/archive/safecom_archive/voip/BSIIntroduction123009_v2.pdf

Appendix D – Compliance Requirements for DHS Grants

This Appendix provides guidance for Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) grants. Recipients using DHS/FEMA funds for emergency communications activities must comply with the *SAFECOM Guidance on Emergency Communications Grants* (*SAFECOM Guidance*) in accordance with DHS Standard Terms and Conditions. Table D-1 provides a list of *SAFECOM Guidance* compliance requirements for DHS/FEMA grants. For additional information, see the relevant sections within *SAFECOM Guidance*. Further, DHS/FEMA recipients should refer to the specific Notice of Funding Opportunity for all programmatic requirements that apply.

Table D-1. SAFECOM Guidance Compliance Instructions for DHS Recipients

Topics	Requirements
National and Statewide Plan Alignment Sections 2.2, 3.1	• Describe in applications how proposed projects will support national goals and objectives in the 2014 National Emergency Communications Plan (NECP). • Describe in applications how proposed projects will align with your State or territory's Statewide Communication Interoperability Plan (SCIP) goals and objectives. To find your SCIP, contact your Statewide Interoperability Coordinator (SWIC) or SCIP Point of Contact. If you do not know your SWIC or SCIP Point of Contact, email the DHS Office of Emergency Communications (OEC). • Confirm submission of the SCIP Annual Snapshot to DHS OEC (via SCIP@hq.dhs.gov) with your State governance and leadership.
Project Coordination Sections 2.1, 2.2, 2.4, 3.2, 3.3	• List all participants involved in project planning to demonstrate engagement with the whole community in accordance with Presidential Policy Directive-8 and NECP's emergency communications ecosystem. • Develop regional, multi-jurisdictional, multi-disciplinary, and cross-border projects to promote greater interoperability across agencies, pool grant resources, facilitate asset-sharing, and eliminate duplicate purchases. • Coordinate proposals with statewide emergency communications governance bodies and leaders (e.g., State Interoperability Executive Committee, SWIC, FirstNet State Single Point of Contact [SPOC], 911 Administrator, or Advisory Board).
National Incident Management System (NIMS) Sections 3.4, 4.3, 4.4	• Report NIMS adoption and implementation in your State Preparedness Report (SPR). The SPR is an annual capability assessment required by any state or territory receiving federal preparedness assistance administered by DHS. States/territories must submit their annual SPR through the Unified Reporting Tool (URT) and email a copy of the URT submission to their respective DHS/FEMA Regional Federal Preparedness Coordinator and copy fema-spr@fema.dhs.gov. Submissions of the SPR are due no later than December 31 each year. • Emergency management personnel shall complete the following training requirements and record proof of completion: NIMS Training, Independent Study (IS) 100, IS 200, IS 700, and IS 800, and other Independent Study courses identified in FEMA Professional Development Series. Previous versions of the IS courses meet the NIMS training requirement. A complete list of Independent Study Program Courses may be found at http://training.fema.gov/is. • FEMA funds used for training should support the nationwide implementation of NIMS. The NIMS Training Program establishes a national curriculum for NIMS and provides information on NIMS courses. Grantees are encouraged to place emphasis on the core competencies as defined in the NIMS Training Program. • NIMS Guideline for Credentialing of Personnel provides guidance on the national credentialing standards. While required for Federal agencies, FEMA strongly recommends State, local, tribal, territorial, and private sector entities also follow.

Spectrum Licensing Section 3.3	• If project requires new spectrum license, consult the appropriate statewide coordinator (e.g., SWIC, FirstNet SPOC), the Federal Communications Commission, and/or FirstNet to ensure the grantee will have authority to operate in the desired spectrum. Spectrum consultation should begin prior to application submission or during early phases of an approved project. A spectrum license must be in place before associated equipment can be purchased.
Planning and Organization Sections 2.2, 3.4, 4.2	• Update and submit the State Preparedness Report and Threat and Hazard Identification and Risk Assessment (THIRA).
Training Sections 2.3, 4.3	• Describe in applications how training projects support the NIMS Training Program, are consistent with NECP priorities, and address gaps identified through your State or territory's SCIP, After-Action Reports, and other assessments.
Exercises Section 2.3, 4.4	• Include participants from multiple jurisdictions, disciplines, and levels of government and private sector entities, as appropriate. For additional FEMA exercise guidance, see http://www.fema.gov/exercise. • Manage and execute exercises in accordance with the Homeland Security Exercise and Evaluation Program.
Land Mobile Radio (LMR) Equipment Sections 2.5, 4.5, 5, Appendix B	• LMR systems are designed to meet public safety's unique mission critical requirements and support time-sensitive, lifesaving tasks, including rapid voice call-setup, group calling capabilities, high-quality audio, and guaranteed priority access to the end-user. For the foreseeable future, the public safety community is expected to follow a multi-path approach to network infrastructure use and development of advanced technologies. Grantees should sustain current LMR capabilities during deployment of advanced technologies in accordance with the NECP. • Select Project 25 (P25) standards-based equipment for LMR mission critical voice communications. See the DHS Authorized Equipment List to determine allowable equipment types for FEMA programs. If proposal includes any non-P25 LMR equipment, grantees must apply for prior approval.
Next Generation 911 Systems Sections 2.5, 4.5, 5, Appendix B	• Next Generation 911 (NG911) is an Internet Protocol (IP)-based system that allows digital information (e.g., voice, photos, videos, text messages) to flow seamlessly from the public through the 911 network and on to emergency responders. If proposal includes NG911 systems, review the NG911 Standards Identification and Review and select IP-enabled 911 open standards equipment and software. For additional information, consult the National 911 Program Office.
Public Safety Broadband Sections 2.5, 4.5, 5, Appendix B	• Each State or territory has designated a State Single Point of Contact to engage FirstNet and serves as the coordinator of the State and Local Implementation Grant Program funds. Consult with the SPOC for the latest guidance from FirstNet, planning for public safety broadband network activities, and identifying the authority to operate on public safety spectrum. To find the FirstNet SPOC for your State or territory, refer to http://firstnet.gov/consultation.
Alerts and Warnings Sections 2.5, 4.5, 5, Appendix	• The Integrated Public Alert and Warning System (IPAWS) is a modernization and integration of the nation's alert and warning infrastructure. Federal, State, local, tribal, and territorial alerting authorities can use IPAWS and integrate local systems that use Common Alerting Protocol standards with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System, Wireless Emergency Alerts, the National Oceanic and Atmospheric Administration Weather Radio, and other public alerting systems from a single interface. If proposal includes alerts and warnings, review IPAWS informational materials and Common Alerting Protocol standard at https://www.fema.gov/informational-materials.