

Office of Emergency Communications:

Fiscal Year 2018

SAFECOM Guidance on Emergency Communications Grants

SAFECOM™

Homeland Security

A Message to Stakeholders

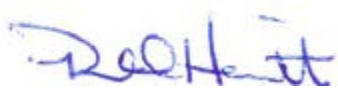
On behalf of the Office of Emergency Communications (OEC), I am pleased to present the *Fiscal Year 2018 SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)*. This document is updated annually to provide current information on emergency communications policies, eligible costs, best practices, and technical standards for state, local, tribal, and territorial grantees investing federal funds in emergency communications projects.

The *SAFECOM Guidance* aligns with the *National Emergency Communications Plan* (NECP), which emphasizes the need to enhance 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 *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. Department of Homeland Security grant recipients investing in emergency communications are still required to comply with *SAFECOM Guidance Appendix D*. All grantees are strongly encouraged to coordinate with their statewide governance bodies 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. These coordination efforts are important to ensure interoperability remains a top priority.

The *SAFECOM Guidance* 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, there is a need to sustain current land mobile radio (LMR) systems into the foreseeable future. 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 integration and deployment of new technologies. Grantees must also consider cybersecurity risks across all capabilities when planning operable, interoperable, and continuity of communications.

As in previous years, OEC developed the *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 emergency communications policies are coordinated and consistent across the Federal Government. OEC encourages grantees to reference this document when developing emergency communications investments, and to direct any questions to my office at oec@hq.dhs.gov.



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

Contents

A Message to Stakeholders 1
Contents 2
1. Introduction 3
1.1 Purpose of SAFECOM Guidance 3
1.2 Report Methodology 4
1.3 Use of SAFECOM Guidance 5
1.4 Key Changes and Updates 7
2. Emergency Communications Priorities 8
2.1 Priority 1: Governance and Leadership 8
2.2 Priority 2: Statewide Planning and Procedures for Emergency Communications 9
2.3 Priority 3: Emergency Communications Training and Exercises 11
2.4 Priority 4: Activities that Enhance Operational Coordination 12
2.5 Priority 5: Standards-based Technology and Equipment 13
3. Before Applying 15
3.1 Review the NECP and SCIP 15
3.2 Coordinate with Statewide Emergency Communications Leaders 15
3.3 Recognize Changes in the Emergency Communications Ecosystem 15
3.4 Understand Federal Grant Requirements and Restrictions 21
4. Eligible Activities 25
4.1 Personnel 25
4.2 Planning and Organization 26
4.3. Training 29
4.4 Exercises 30
4.5 Equipment 31
5. Emergency Communications Systems and Capabilities 36
6. Grants Management Best Practices 37
7. Funding Sources 38
Appendix A – Acronym List A-1
Appendix B – Technology and Equipment Standards B-1
Appendix C – Emergency Communications Resources C-1
Appendix D – Compliance Requirements for DHS Grants D-1

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 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)* as a reference guide for entities applying for federal financial assistance for emergency communications projects. While only entities funding emergency communications projects with DHS grant funding are required to comply with *SAFECOM Guidance* (see Appendix D), all entities are highly encouraged to follow the recommendations within this document to ensure interoperable, resilient, and fully effective communications. 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] It 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 DHS Office for Interoperability and Compatibility also 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, technical support, 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 SAFECOM Guidance

The *SAFECOM Guidance* provides guidance to grant recipients[5] on:

- Recommendations for planning, coordinating, and implementing projects
- Emergency communications activities that can be funded through federal grants
- Best practices, policies, and technical standards that help to improve interoperability
- Resources to help grantees comply with technical standards and grant requirements

[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 ECPC Grants Focus Group is comprised of grant officers, program administrators, and communications experts representing the 14 federal agencies that participate in the ECPC.
[5] In accordance with Title 2 of the Code of Federal Regulations (CFR) 200, the terms "recipient" and "sub-recipient" is defined as a non-federal entity that receives a federal award directly from a federal awarding agency to carry out an activity under a federal program.

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 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 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 network
- Enhancing coordination among stakeholders, processes, and planning activities across the broader emergency response community

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).[6] Best practices and technical standards located within the *SAFECOM Guidance* help ensure federally-funded emergency communications investments are interoperable, fully effective and reliable, and support 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, grant applicants and recipients should review specific grant guidance carefully to ensure their proposed activities are eligible, and all standards, terms, and conditions required by the program are met.[7]

1.2 Report Methodology

OEC consulted with federal, state, and local partners to develop the *SAFECOM Guidance*, including the priorities, recommendations, and technical standards. Priorities within this document represent current needs and initiatives that stakeholders and federal partners have recognized as integral to emergency communications and recommended to continue funding in FY 2018. 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[8]
- U.S. Department of Agriculture (USDA)
- U.S. Department of Commerce
    - First Responder Network Authority (FirstNet)
    - National Telecommunications and Information Administration (NTIA)

[6] For information on SCIPs, see the OEC website at: http://www.dhs.gov/statewide-communication-interoperability-plans.
[7] 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.
[8] 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.

- U.S. Department of Homeland Security
  - Federal Emergency Management Agency (FEMA)
  - 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 SAFECOM Guidance

The *SAFECOM Guidance* should be used during 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 *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 available to recipients.

Table 1. Essential Resources for Emergency Communications Grant Recipients

Resources	Descriptions
National Emergency Communication Plan	The NECP is the only strategic national 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 investments support the goals and objectives of the Plan. The NECP is available at: http://www.dhs.gov/necp.
Statewide Communication Interoperability Plan	The SCIP contains the state, territory, or tribal government'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 reports annually on the progress of the state or territory 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 Statewide Interoperability Coordinator (SWIC) to ensure 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.
IPAWS Website	This website contains information on IPAWS's capabilities, who can use IPAWS to send alerts and warnings, and organizations that work with the IPAWS Program Management Office to support public alerts and warnings. IPAWS is accessed through software that meets IPAWS system requirements. There is no cost to send messages through IPAWS, although there may be costs associated with acquiring compatible alert origination software. Grantees are encouraged to invest in alerting software. IPAWS is not mandatory and does not replace existing methods of alerting, but instead complements existing systems and offers new capabilities to deliver timely and actionable alerts. See the IPAWS website at https://www.fema.gov/integrated-public-alert-warning-system and specific information for alerting authorities at https://www.fema.gov/alerting-authorities.

Resources	Descriptions
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/.
Statewide Interoperability Coordinator	States, territories, and tribal governments are encouraged to designate a full-time **SWIC** who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government. Grant applicants are strongly encouraged to coordinate project proposals with the SWIC to ensure projects support statewide efforts to improve emergency communications. To find your SWIC, contact OEC at: oec@hq.dhs.gov.
State Leadership	As required as a condition of the State and Local Implementation Grant Program (SLIGP) and SLIGP 2.0, each State and Territory Governor designated an individual or body to serve as coordinator for SLIGP and SLIGP 2.0. Grantees are encouraged to consult with the appropriate governance body for their state or territory when engaging in public safety broadband activities. The **State Emergency Management Agency Director** is responsible for ensuring 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, 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. Grantees are encouraged to coordinate 911 projects with the Administrator to ensure projects support state or territory 911 efforts. To find your 911 Administrator, refer to the National Association of State 911 Administrators 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 Director or office, refer to: http://www.dhs.gov/state-homeland-security-contacts.
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 FirstNet. 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 the network. 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. Grantees are encouraged to coordinate 911 projects with the Board to ensure projects support state or territory 911 efforts. To find your 911 Advisory Board, refer to State 911 Contacts page of the National Association of State 911 Administrators at: http://www.nasna911.org/state-911-contacts.

1.4 Key Changes and Updates

This section highlights key changes to the *FY 2018 SAFECOM Guidance*:

- **Emergency Communications Priorities (Section 2).** This section reviews the FY 2018 priorities including: Governance and Leadership, Statewide Planning and Procedures for Emergency Communications, Emergency Communications Training and Exercises, Activities that Enhance Operational Coordination, and Standards-based Technology and Equipment. Based on lessons learned from recent federal disasters, there is an urgent need to address communications survivability, resilience, and continuity. Rather than listing this as a separate priority, communications resilience and continuity should be viewed as a critical component across all priorities.

- **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 applicants should consider before applying.

- **Eligible Activities (Section 4).** This section includes a review of eligible costs and guidance for applicants 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 applicants 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 recipients can reference when developing emergency communications projects. In Appendix D, DHS has outlined specific requirements for DHS/FEMA recipients to comply with *SAFECOM Guidance*. These requirements are in accordance with the DHS Standard Terms and Conditions of preparedness grants.

2. Emergency Communications Priorities

OEC is responsible for ensuring grant guidelines and priorities relating to interoperable emergency communications are coordinated and consistent with the goals and recommendations in the NECP.[9] In support of this mandate, the *FY 2018 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. Grantees are encouraged to target grant funding toward the following priorities:

- Priority 1: Governance and Leadership
- Priority 2: Statewide Planning and Procedures 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 change 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 2018, grant recipients are encouraged to invest in emergency communications governance and leadership structures for coordinating statewide and regional initiatives that reflect the evolving emergency communications environment.[10] 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.[11]

To support this priority, grantees should target funding to:

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

[9] 6 U.S.C. §574.

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

[11] See the *National Incident Management System Implementation Objectives* at: http://www.fema.gov/national-incident-management-system.

- Include and coordinate with emergency communications leaders (e.g., 911 leaders, IPAWS Program Management Office, Regional Emergency Communications Coordination Working Groups [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 post-State Plan period and radio access network buildout, 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
- Develop governance to aid in coordination of messaging within partnering IPAWS Alerting Authorities; improve the common operating picture; and create awareness of existing plans, policies, and procedures

2.2 Priority 2: Statewide Planning and Procedures for Emergency Communications

The emergency communications community benefits from a comprehensive and inclusive approach to planning. The 2014 NECP recommends that response agencies seek to improve responders' ability to communicate and share information with others through increased strategic planning, the adoption of standard operating procedures (SOP) that integrate the capabilities of all users, and regular training and exercises. Through development and updating of their SCIPs, states, tribes, and territories engage multiple jurisdictions, disciplines, and levels of government in planning, 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 SOPs 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 agencies to effectively identify, prioritize, and coordinate to ensure proposed investments support statewide, tribal-wide, and territory-wide planning priorities.

In FY 2018, grant recipients should continue to target funding toward planning activities, including updates of statewide, tribal-wide, and territory-wide plans, and ensure plans incorporate the capabilities and needs of all emergency communications systems. The goal of this priority is to ensure emergency communications needs are continually assessed and integrated into risk assessments and preparedness plans, including continuity planning efforts. These planning activities must include analyzing threats and vulnerabilities that may affect communications resilience and developing investment plans and SOPs to mitigate identified risks. Stakeholders are encouraged to target 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, grant recipients 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 whole community concepts[12]
  - Address findings and gaps identified in state-level preparedness reports, risk and vulnerability 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., narrowbanding, 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 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),[13] and state-level planners (e.g., 911 planners, utilities commissions) to ensure proposed investments align to statewide plans and comply with technical requirements
- Identify, review, establish, and improve SOPs in coordination with response agencies at all levels of government to:
  - Ensure federal, state, local, tribal, and territorial roles and responsibilities are clearly defined
  - Ensure communications assets and capabilities are integrated, deployed, and utilized to maximize interoperability
  - Address threats and vulnerabilities and identify contingencies for the continuity of critical communications
- Establish a cybersecurity plan including continuity of vulnerable communications components, such as Radio Frequency (RF)-based communications that do not rely on public infrastructure

[12] 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."

[13] Many federal grants are awarded to a designated SAA as the official recipient and administrator for the grant, responsible for sub-recipient oversight of grant-funded activities.

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 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. The NECP recommends agencies involve responders from all levels of government, as well as non-governmental stakeholders, to practice a whole community response. It also recommends agencies utilize all types of communication technologies, and identify gaps and problems with technologies or protocols.

In FY 2018, grant recipients should continue to invest in emergency communications-related training and exercises to address gaps identified in response and recovery operations, which should include thoroughly testing resiliency and continuity of communications. 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, grant recipients 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])[14]
- Improve states', tribal, 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)
- Conduct frequent training and exercises involving personnel from all levels of government who are assigned to operate communications capabilities
- 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 to include tribes
- Provide training and exercises on new and existing systems, equipment, and SOPs
- Test communications survivability, resilience, and continuity of communications
- 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
- Provide regular training and exercises for IPAWS Alerting Authorities incorporating the use of IPAWS

[14] 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: https://www.fema.gov/training-0.

2.4 Priority 4: Activities that Enhance Operational Coordination

There has been significant improvement in capabilities at state local, tribal, and territorial levels resulting in the ability of jurisdictions to more effectively coordinate communications resources and services during emergencies. This includes integration of capabilities, resources, and personnel across the whole community. As incidents escalate, communications resources must be able to expand rapidly to meet responders' needs. This requires agencies to track communications resources they own or can access, then follow appropriate procedures to request and deploy resources to locations when needed.

In FY 2018, grant recipients are encouraged to update inventories of communications assets and share information within their state, tribe, or territory and region (e.g., neighboring states, tribes, or territories) that are most likely to request support during emergencies or events. This can be achieved by working with SWICs to update 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.[15] Grant applicants and recipients should identify gaps in capabilities and target funding toward those gaps. In addition, grantees must continue to implement NIMS ICS principles during all emergencies. Grant applicants and recipients are also encouraged to actively engage neighboring jurisdictions—both internal and external to the state tribe, or territory—to coordinate response planning and seek mutual aid agreements for large-scale responses. Agencies should also collaborate and encourage alerting practices between levels of government including installing resilient communications to coordinate the distribution of alerts.

To support this priority, grant recipients 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 Tool)
- Conduct risk and vulnerability assessments
- 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 and address continuity of communications
- 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, cell on wheels)
- Address needs identified in statewide plans, AARs, or assessments
- Support communications initiatives that engage the whole community

[15] 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.

2.5 Priority 5: Standards-based Technology and Equipment

The public safety community relies on LMR as its primary source for mission critical voice communications. As a result, agencies have prioritized maintaining LMR systems and equipment to deliver public safety requirements for interoperability, security, and reliability. Agencies are also adopting Internet Protocol (IP)-based technologies and services for data access and transmission. This integration of technologies presents new challenges, such as cybersecurity; therefore, agencies must improve understanding and preparations for security risks associated with IP-based communications systems. This requires 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.[16]

In FY 2018, grant recipients 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 applicable standards. Grant recipients are strongly encouraged to invest in equipment that will 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 should participate in community outreach and planning to ensure new capabilities are interoperable and all user requirements are incorporated.

To support this priority, grant recipients should target funding to:

- Sustain and maintain current LMR capabilities
- Purchase and use Project 25 (P25) compliant LMR equipment (see P25 Compliance Assessment Program [CAP] approved equipment list) for mission critical voice communications[17]
- Support rapid deployment of the Nationwide Public Safety Broadband Network (NPSBN) and use of FirstNet device and application portfolio dedicated for public safety using multi-layered, proven cybersecurity and network security solutions[18]
- Meet FCC and FirstNet technical and eligibility requirements for the network
- Transition towards Next Generation 911 (NG911) capabilities
- Require or encourage compliance with NG911 standards for grant funded projects
- Support standards that allow for alerts and warnings across different systems
- Secure equipment, information, and capabilities from physical and virtual threats
- Acquire, sustain, and maintain Common Alerting Protocol compliant software that meets IPAWS system requirements
- Sustain and ensure critical communication systems connectivity, including backup solutions, among key government leadership, internal elements, other supporting organizations, and the public under all conditions

[16] 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.

[17] For more information on P25 requirements, see: http://www.project25.org/. For a list of P25 CAP approved equipment, see: https://www.dhs.gov/science-and-technology/p25-cap-grant-eligible-equipment.

[18] Applicants interested in broadband investments should consult with FirstNet to ensure investments meet all technical requirements to operate on the network. Please refer to FirstNet's contact information at: http://www.firstnet.gov/.

- Ensure all communications systems and networks are traced from end-to-end to identify all Single Points of Failure, including redundancy at critical infrastructure facilities, and:
  - Sustain availability of backup systems (e.g., backup power, portable repeaters, satellite phones, High Frequency [HF] radios)
  - Ensure diversity of network element components and routing
  - Plan for geographic separation of primary and alternate transmission media
  - Maintain spares for designated critical communication systems
  - Work with commercial suppliers to remediate Single Points of Failure
  - Maintain communications capabilities to ensure their readiness when needed

3. Before Applying

Before applying for federal funds for emergency communications, applicants 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

Grant applicants should read the NECP to understand the national emergency communications strategy, and to ensure proposed projects support national goals and objectives. Similarly, grantees should review their state or territory's SCIP to ensure proposals support statewide plans to improve communications across all emergency communications systems and capabilities.[19]

In addition to developing and updating SCIPs, OEC requests 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 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., 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.

[19] For a copy of the 2014 NECP, see: https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf.

Developments in Advanced Technologies[20]

Traditionally, LMR systems were the primary capabilities the public safety community used to achieve mission critical voice communications in the field. 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 NG911, an IP-based model that will enable increased resilience and redundancy in call routing, as well as 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 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. Grant recipients 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. The public safety community continues to rely on LMR as its primary source to achieve mission critical voice communications in the field.

[20] 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 of 2012, the IPAWS Modernization Act of 2015, 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 strategies, resource decisions, and investments for emergency communications keep pace with the evolving environment, and 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.[21]

  Grantees should read the 2014 NECP to understand the national emergency communications strategy, and to ensure 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 of 2012.*** Signed into law on February 22, 2012, the Act established FirstNet, an independent authority within NTIA, and directed it to ensure the establishment of the NPSBN.[22] The Act reallocated and designated 700 MHz D Block spectrum for public safety use to FirstNet.[23] FirstNet engaged in comprehensive outreach and consultation efforts with public safety entities in federal, state, local, tribal, and territory jurisdictions to plan for the network. FirstNet 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 network. The FirstNet network solution will be based on a single, national network architecture that evolves with technological advances and initially consists of a core network and a radio access network (RAN).[24]

  FirstNet operates under a services-based model where eligible users subscribe to a level of service that aligns with their mission needs. The principle responsibility of federal, state, local, tribal, and territorial public safety entities will be the acquisition of authorized and compatible devices and applications that operate on the network and determination of connectivity for any locally maintained databases that will support public safety operations. Infrastructure and maintenance costs of the network core and RAN will be borne by FirstNet.

[21] For more information on the NECP, see: http://www.dhs.gov/necp.
[22] For more information on the Act, see: http://www.ntia.doc.gov/category/public-safety.
[23] 47 U.S.C.§ 1421(a).
[24] 47 U.S.C. § 1422(b).

Per the Act, FirstNet delivered final State Plans to Governors to make an Opt-in/Opt-out decision. All 50 States, 5 Territories, and the District of Columbia have chosen to Opt-in to the FirstNet solution and will have a FirstNet network presence in accordance with the State Plan.

At this time, grantees would be best served by acquiring long-term evolution (LTE) devices or network equipment only after receiving further guidance from FirstNet on the technical requirements of and compatibility with the network. Additional outreach and planning activities (e.g., community outreach and education, documenting user needs) that support the arrival of public safety broadband technologies should be done in consultation with FirstNet.

Grantees interested in investing federal funds in broadband-related projects should consult with FirstNet and the federal granting agency to understand all requirements impacting broadband investments. FirstNet, with their network partner is the sole nationwide licensee for Band 14 spectrum and the FirstNet Authority does not anticipate entering into any other spectrum agreements. 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.[25]

- ***IPAWS Modernization Act of 2015.*** Signed into law in April 2016, Public Law 114-143 calls for the modernization of IPAWS to ensure the President can communicate under all conditions, establishes a Subcommittee to the National Advisory Council composed of IPAWS stakeholders to expand collaboration and recommend improvements to the system, and requires annual performance reports.[26] The Act includes 19 additional system and implementation requirements, which the program is currently evaluating and estimating the resources necessary to fulfill to the extent feasible.

- ***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: *National Preparedness Goal*; National Preparedness System; *National Preparedness Report*[27]; and the Campaign to Build and Sustain Preparedness. The directive emphasizes that national preparedness is the shared responsibility of the whole community.[28]

[25] 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.
[26] For more information on the IPAWS Modernization Act of 2015, visit: https://www.congress.gov/bill/114th-congress/senate-bill/1180.
[27] 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.
[28] For more information on PPD-8, see: http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

As a result, many grants that fund emergency communications now require grantees to engage the whole community in planning. FY 2018 federal grant programs will require grant applicants 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, which in turn improves preparedness and response.

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 license for the 700 MHz public safety broadband spectrum to build and operate the network. Grantees seeking federal funds for emergency communications projects should be aware of several federal initiatives and actions affecting spectrum use for public safety entities. Grantees should review the following spectrum issues, confirm their proposed projects are consistent with regulatory requirements and initiatives, and consult the appropriate coordinator (e.g., Frequency Coordinator, SWIC), 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**.[29] The FCC mandated 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 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.[30]

- **800 MHz Reconfiguration (Rebanding).**[31] 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 their 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.[32] The

[29] For more information on narrowbanding, see: http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html.
[30] 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.
[31] For more information on 800 MHz reconfiguration, see: http://www.800ta.org/.
[32] T-Band markets 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.

Act requires the FCC to commence the auction process 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 providing T-Band incumbents commit to return an equal amount of T-Band channels priority access to the 700 MHz Narrowband Reserve Channels for a five-year period.[33] Grantees seeking funding for relocation of T-Band systems should consult the FCC,[34] SWIC, and a frequency coordinator[35] 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.**[36] 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 operating in this band had to migrate from the band to clear the spectrum for NPSBN use by August 31, 2017.[37] FirstNet established a grant program to support such relocation by qualified licensees. FirstNet provided relocation grant awards to ten narrowband incumbents totaling more than $27.3 million. While a majority of incumbents have cleared the spectrum by the deadline, several incumbents were provided no-cost extensions and continue to move forward in clearing the spectrum. Grantees operating in the 700 MHz public safety broadband spectrum should consult with their appropriate governance entity during this transition.

In general, grantees should consult with the regulatory agency and 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.[38] 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,[39] 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[40]
- Reprogramming existing equipment to comply with spectrum migration

Reduction and Streamlining of Grants

[33] For more information, see FCC 14-172 at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-172A1.pdf.
[34] Grantees can contact the FCC Public Safety and Homeland Security Bureau at: pshsbinfo@fcc.gov.
[35] For more information on frequency coordinators, see: http://transition.fcc.gov/pshs/public-safety-spectrum/coord.html.
[36] The public safety broadband spectrum band is 763-768 MHz and 793-798 MHz.
[37] Any incumbents that wished to remain on FirstNet's spectrum after August 31, 2017, had to obtain FirstNet's consent to do so.
[38] Contact the FCC's Public Safety Homeland Security Bureau at pshsbinfo@fcc.gov and FirstNet at outreach@firstnet.gov.
[39] Generally, federal licensing fees are *not* allowable under most federal grants; however, applicants 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/.
[40] Some federal grants do not allow construction or ground-disturbing activities. Consult the grant officer on these activities.

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 communications needs into statewide plans and to ensure communications projects are prioritized by states and territories. Grant applicants are encouraged to:

- Coordinate projects with the SWIC, 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[41]
- Leverage assessment data to develop strong statements of need that can be shared with state leaders responsible for prioritizing projects for funding[42]
- Identify additional sources of funding for emergency communications improvements[43]

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. Grant applicants 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, recipients should be aware of common requirements for grants funding emergency communications,[44] including:

- **Environmental Planning and Historic Preservation (EHP) Compliance.** Recipients must comply with all applicable EHP laws, regulations, Executive Orders, and agency guidance. Recipients are strongly encouraged to discuss projects with federal grant

[41] Applicants should work with SWICs and the FCC to ensure 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/. 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. Recipients should work closely with grant officers on these projects.

[42] Applicants 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.

[43] For additional sources of funding, see the *List of Federal Financial Assistance Programs Funding for Emergency Communications* posted to the SAFECOM website at: http://www.dhs.gov/safecom/funding.

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

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 response, and to receive preparedness grant funding. State, local, tribal, and territorial recipients should ensure the most recent NIMS reporting requirements have been met.[45]

- **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.

- **Threat and Hazard Identification and Risk Assessment (THIRA).** In FY 2018, DHS/FEMA is requiring Homeland Security Grant Program, Tribal Homeland Security Grant Program, and Emergency Management Performance Grant Program recipients 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.[46] 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 2018 Notice of Funding Opportunity (NOFO) for grant-specific THIRA requirements and impact on annual grant funding.[47]

- **Authority to Operate.** In establishing requirements for the NPSBN and providing 20 MHz of the upper 700 MHz spectrum to FirstNet, Congress directed 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 holds a single nationwide FCC license for the combined public safety broadband spectrum (763-768 MHz and 793-798 MHz) and D Block spectrum (758-763 MHz and 788-793 MHz), commonly referred to as Band 14. The FirstNet license also incorporates two one-MHz guard bands at 769 and 799 MHz. Recipients that have not entered into a spectrum management lease agreement (SMLA) do not have authority to operate in the designated FirstNet spectrum. Accordingly, recipients that do not have access to the designated FirstNet spectrum should not use federal financial assistance to support acquisition-based or deployment-based broadband

[45] The National Integration Center 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.

[46] 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.

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

projects until such time as they have received the necessary authority to operate in the designated FirstNet spectrum. Recipients that have authority to operate may submit projects for funding provided that the request is consistent with the terms and conditions of its SMLA with FirstNet. Recipients 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 network.

- **Reporting.** Federal agencies are improving how they demonstrate impact and effectiveness of federal grant programs.[48] As a result, recipients may be required to report project-level information, performance measurement data, detailed financial reports, and progress reports. Recipients are encouraged to use existing documentation and data (e.g., SCIPs, AARs, assessments) to measure performance and demonstrate how gaps in capabilities will be/were addressed through federal grant funding. Recipients 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

Recipients should ensure 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

Recipients should be aware of common restrictions on federal grant funding and should consult the grant 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. Recipients must ensure federal funds are used for purposes that were proposed and approved, and have financial systems in place to properly manage grant funds. Recipients cannot commingle federal sources of funding. The accounting systems of all recipients and sub-recipients must ensure federal funds are not commingled with funds from other awards or federal agencies.

- **Cost Sharing/Matching Funds.** Recipients must meet all matching requirements prescribed by the grant. If matching funds are required, 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

[48] 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. Recipients are encouraged to develop a plan to sustain critical communications positions in the event 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 recipients 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.[49] Grant applicants 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. However, applicants should note all activities listed in this section may not be eligible for funding under all grant programs. Applicants should read each grant guidance and related information carefully to ensure activities proposed are eligible under the program before developing or submitting applications.

4.1 Personnel

Many federal grants allow recipients to hire full- or part-time staff, contractor staff, or consultants to assist with emergency communications planning, training, and exercise activities.[50] Allocating funding toward personnel helps ensure grants and grant-funded projects are managed, state-level planning meetings are attended, 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
    - Promote cross-training and continuous training to address changes in the workforce
    - Ensure personnel are proficient in using existing and new technologies

[49] 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. Applicants should be aware that emergency communications personnel, planning, and organizational costs are often allowable under the Planning cost category for grants.

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

- Develop exercises to test training
- Support training conferences
- Develop and implement a curriculum covering technical issues raised by broadband and other advanced technologies
- Address continuity of operations planning requirements
- 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

Grant recipients should be aware of common restrictions on federal grant funding for emergency communications personnel.

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

- **Overtime.** Some federal grants permit the use of funds for overtime related to training. These expenses are limited to 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 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. Recipients should ensure grant funds can be used for overtime and consult their grant officer to correctly calculate overtime costs.

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 plans
    - Disaster emergency communications plans
    - Communications system life cycle planning, including migration planning and use of the *Emergency Communications System Life Cycle Planning Guide* and *Life Cycle Planning Tool*[51]
    - Plans for narrowband conversion and compliance
    - Plans for broadband integration with broader communications capabilities
    - 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 continuity of communications, including backup solutions, if primary systems or equipment fail (e.g., contingency and strategic planning)
    - Planning for training and exercises
    - Identifying security measures for communications networks and systems
    - Planning activities for the transition of 911 to NG911

- **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 the development and sustainment of core capabilities are not exclusive to any single level of government or organization, but rather require combined efforts of the whole community.[52] 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, and managing of emergency communications initiatives. Grant

[51] For more information on the *System Life Cycle Planning Guide*, see: https://www.dhs.gov/publication/funding-documents.
[52] Core capabilities include Prevention, Protection, Mitigation, Response, and Recovery, and are further defined in the *National Preparedness Goal* on the FEMA website at: https://www.fema.gov/national-preparedness-goal.

funds may be used to establish, update, or enhance statewide, regional (e.g., multi-state, multi-urban area), or local 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
- Developing SOPs or templates to provide access to and use of resources
- Continued broadband planning and coordination efforts
- 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., updating the CASM NextGen Tool, creating fleet maps)
  - SOPs, coordination of interoperability channels, and regional response plans
  - Training and exercises
  - Narrowband compliance capabilities and system coverage analysis
  - 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
  - Developing plans to optimize broadband use in support of public safety operations
  - Continued collection of broadband usage data, use cases, and needs analyses
  - Preliminary planning for advanced technologies (e.g., alerts and warnings, NG911)
  - Conducting assessments of cyber risks and strategies to mitigate vulnerabilities before the deployment of IP-based networks
  - Implementing identity, credential, and access management (ICAM) solutions to address growing data management, interoperability, and cybersecurity challenges, with consideration for federated solutions, such as the *Trustmark Framework*[53]

[53] For more information on ICAM and the *Trustmark Framework*, see: https://www.dhs.gov/safecom/icam- resources.

- **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,[54] 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 IPAWS,[55] which consists of:
    - Emergency Alert System
    - Wireless Emergency Alerts
    - IPAWS All-Hazards Information Feed
    - National Oceanic and Atmospheric Administration All Hazards Weather Radio / HazCollect

Additional Requirements and Recommendations for Planning Activities

Additional activities in support of federal planning initiatives include updating and submitting a SPR, THIRA, and SCIP Annual Snapshot, as well as demonstrating 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 public safety officials can achieve mission critical voice communications. As other communications technologies become integrated into response operations, the need for training becomes even more critical to ensure response personnel are maximizing the benefits that new capabilities provide. Training projects should be consistent with the NECP priorities and address gaps identified through SCIPs, TICPs, AARs, and other assessments. Training reinforces SOPs and proper equipment use by personnel. Grantees are strongly encouraged to include training in projects that involve new SOPs or equipment purchase.

- **Development, delivery, attendance, and evaluation of training.**[56] 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:

---

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

[55] The *2017 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 IPAWS, see: https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/1475780581312-b64afc45df4d350873701d6501186e8e/FY2017IPAWSSupplemental10252016.pdf.

[56] DHS training catalogs are available at: https://www.dhs.gov/training-technical-assistance. The federal-sponsored and state-sponsored course catalogs can be found at: https://www.firstrespondertraining.gov.

- Use of SOPs and other established operational protocols (e.g., common language)
- NIMS/ICS training
- COML, COMT, or ICS Communications Unit position training
- Use of equipment and advanced data capabilities (e.g., voice, video, text)
- Disaster preparedness
- Peer-to-peer training
- Regional (e.g., multi-state, multi-urban area) operations
- Population of CASM NextGen Tool
- Integration of broadband devices and applications into public safety operations
- Cyber education on proper use and security of devices and applications, phishing, malware, other potential threats, and how to stay on guard against attacks
- Evaluation and testing of public alert and warning procedures

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

Additional Requirements and Recommendations for Training Activities

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

- **Compliance with NIMS.**[57] State, local, tribal, and territorial entities must adopt NIMS as a condition of many federal grants. Given that implementation of NIMS requires certain training courses, recipients may target funding towards NIMS-compliant training.

- **Completion of Communications Unit Leader Training.** OEC, in partnership with FEMA, the Office for Interoperability and Compatibility, the National Integration Center, 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. Recipients should target grant funding toward this training to improve on-site communications during emergencies, as well as satisfy NIMS training requirements.

4.4 Exercises

Exercises should be used to 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, officials from colleges and universities, and other disciplines and private sector entities, as appropriate. Findings from exercises can be used to update programs to address gaps in emergency communications and emerging technologies, policies, and partners. Recipients are encouraged to increase awareness and availability of emergency communications exercise opportunities across all levels of government.

[57] 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.

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:
  - Use of new or established operational protocols, SOPs, and equipment
  - Regional (e.g., multi-state, multi-jurisdictional) participation
  - Integration of broadband services, devices, and applications into public safety operations

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

Additional Requirements and Recommendations for Exercise Activities

Recipients 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.[58]

- **Compliance with NIMS.** HSPD-5 requires all federal departments and agencies to adopt NIMS and use it in their individual incident management programs and activities, including all preparedness grants. DHS/FEMA recipients should review NIMS requirements at: https://www.fema.gov/national-incident-management-system, and ensure 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 appropriate entities (e.g., public safety, utilities, private sector, federal agencies) and resources (e.g., deployable assets).

4.5 Equipment

Emergency management and 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.

[58] HSEEP resources are available at: https://www.preptoolkit.org/web/hseep-resources. For the full HSEEP library, visit: https://www.hsdl.org.

***Eligible Expenses*[59]**

- **Design, construction,[60] implementation, enhancement, replacement, and maintenance of emergency communications systems and equipment, including:**
  - System engineering requirements
  - As-is and proposed enterprise architectures
  - Interoperability verification and validation test plans
  - System life cycle plans
  - Analysis and monitoring of cybersecurity risks
  - Migration to approved, open architecture, standards-based technologies
  - Integration of existing capabilities and advanced technologies (e.g., multi-band/multi-mode capable radio, Internet of Things devices, artificial intelligence, machine intelligence, and data science solutions)
  - Project management costs associated with systems and equipment
  - 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

- **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. Recipients should ensure 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 emergency communications systems.**
  - Installing or expanding battery backup, generators, or fuel systems
  - Evaluating existing shelter space for 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 for additional communications equipment
  - Analyzing physical site security provisions for upgrades and enhancements (e.g., fences, lighting, alarms, cameras, shelter access hardening, protective measures)
  - Evaluating Public Safety Answering Points and other 911 infrastructure sites to determine hardware and software upgrades

[59] While the activities listed are generally allowable for traditional LMR investments, these activities may be restricted for broadband-related investments. Applicants 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.

[60] 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 applicable EHP requirements to select construction-related activities in this guidance.

- **Upgrading connectivity capabilities for 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 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
    - Existing gaps in capabilities, connectivity, coverage, or application support

- **Purchase of:**
  - Standards-based interoperable communications equipment listed on the Authorized Equipment List (AEL)[61]
  - P25 complaint radio equipment listed on the P25 CAP Approved (Grant-Eligible) Equipment List[62]
  - Broadband user equipment, applications, and services, which are compliant with the NPSBN
  - 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)
  - Alerts and warnings software that is compliant with the Common Alerting Protocol standards, user friendly, and meets IPAWS system requirements

Additional Requirements and Recommendations for Equipment Purchases

Recipients should anticipate additional requirements when purchasing equipment with federal grant funds, including:

[61] For a list of equipment typically allowed under DHS/FEMA grants, see: http://www.fema.gov/authorized-equipment-list.
[62] For a list of P25 compliant radio equipment, see: https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment.

- **Assignment of full-time Statewide Interoperability Coordinator.** In FY 2018, DHS/FEMA will require all states and territories receiving Homeland Security Grant Program funds to designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government. Responsibilities include establishing and maintaining statewide plans, policies, and procedures, and coordinating decisions on communications investments funded through federal grants. SWIC status information will be maintained by OEC and verified by FEMA through programmatic monitoring activities for DHS/FEMA grant recipients.

- **Coordination with statewide emergency communications leaders.** Recipients are strongly encouraged to coordinate with the SWIC, other emergency communications governance bodies and leadership, and appropriate state, local, tribal, and territorial partners to ensure consistency with statewide plans, and compatibility among existing and proposed emergency communications systems.

- **Compliance with technical standards.** DHS/FEMA recipients must ensure all grant-funded equipment complies with technical standards in the *SAFECOM Guidance Appendix B*, unless otherwise noted in a program's grant guidance.[63] Other federal grants require recipients to explain how their procurements will comply with applicable standards for LMR, IP-based systems, and alert and warning systems or provide compelling reasons for using non-standards-based solutions. Recipients 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 planned operations or if a waiver is needed. Grantees can contact the FCC at PSHSBinfo@fcc.gov.

- **Compliance with federal EHP laws and policies.** Recipients must ensure federally-funded projects comply with relevant EHP laws. Construction and 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. Recipients should discuss proposed construction-related activities with federal granting agencies *before* beginning work to determine whether proposed activities are allowed, and to determine if proposed activities are subject to EHP review.[64]

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

---

[63] Technical standards and requirements vary among federal grant programs (especially grants funding research and testing). Applicants should review grant guidance to ensure 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.

[64] 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://energy.gov/sites/prod/files/NEPA-40CFR1500_1508.pdf.

- **Sustainment of current LMR capabilities.** Grantees are strongly encouraged to sustain current LMR capabilities for mission critical voice capabilities so that systems continue to deliver reliable communications.[65]

- **Compliance with federal procurement requirements.** As a condition of funding, recipients agree to comply with federal procurement requirements. Recipients are responsible for ensuring open and competitive procurements, subject to the specific programmatic requirements of the grant, and applicable state or local procurement requirements. Recipients 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
    - Recipients/sub-recipients should avoid non-competitive practices (e.g., contractors that developed the specifications for a project should be excluded from bidding)
    - Recipients/sub-recipients 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 recipients to submit system life cycle plans for equipment purchased with federal grant funds.[66] As a result, recipients 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.

[65] For guidance on funding and sustainment of LMR capabilities, see: http://www.dhs.gov/safecom/funding.
[66] For guidance on system life cycle planning, see: https://www.dhs.gov/safecom/resources-library.

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 LMR will remain an important tool for mission critical voice communications for emergency responders in the field for many years to come. Successful future planning 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 become integrated with one another, interoperability and cybersecurity become increasingly important. When procuring equipment or software for emergency communications systems, grantees are strongly encouraged to 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	• Review the P25 technical standards for LMR • Specify applicable P25 standards and specifications in the P25 Steering Committee list of approved standards. For the list of current P25 standards, see: http://www.ptig.org • Select P25 Compliance Assessment Program (CAP) approved equipment • Obtain documented evidence of P25 CAP compliance; in the absence of testing information on the P25 Compliance Assessment Bulletins, entities should request results of applicable test procedures identified in the P25 standards list • Ensure additional features purchased are P25 compliant (e.g., AES 256 encryption) • Ensure non-standard features are identified and understand impact on interoperability • Provide written justification for non-compliant P25 purchases
Next Generation 911	• Read the *NG911 Standards Identification and Review*[67] 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 FirstNet for guidance on how to best incorporate broadband communications into a public safety entity's communications ecosystem • Plan backhaul, application software, and IT infrastructure upgrades to connect enterprise networks to FirstNet
Data Information Sharing	• Evaluate data information sharing needs and standards based on existing systems, users, and the type of information being exchanged • 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
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[68] • Complete the IPAWS Memorandum of Agreement process

[67] For a copy of the *NG911 Standards Identification and Review*, see: https://www.911.gov/standardsfornextgen.html.
[68] For information on CAP and IPAWS, see: https://www.fema.gov/integrated-public-alert-warning-system.

6. Grants Management Best Practices

Proper management of grants enables recipients 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 recipients 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 the SWIC and other key governance bodies and leadership to document needs, align projects to plans, and identify funding options[69] • Work with SAA to include projects in state preparedness plans and to secure funding • Review program 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-recipients 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 closeout, 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 impacting progress or spending • 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 closeout reports; report on final performance

[69] Stakeholders can also contact their respective Regional Coordinator for guidance.

7. Funding Sources

Applicants should consider all available funding sources, including traditional grants to help fund initial capital investments or improvements to communications systems, 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 ECPC Grants Focus Group, OEC identified 21 federal grants and loans that fund emergency communications.[70] 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 funding sources

Other Sources of Federal Funding

While the *SAFECOM Guidance* 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 provided critical funding for emergency communications projects.[71] While loans offer an alternative to traditional grants, grantees should work with financial experts to understand loan terms and ensure their proposals meet all requirements under each program.

Also, there are several federal programs that are not solely focused on 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 funding sources, such as rural grants and loans, and work with eligible entities for those programs to improve communications infrastructure.

[70] For an updated list of federal grants and loans that fund emergency communications, see: http://www.dhs.gov/safecom/funding. Applicants can find and search grants and loans at: http://www.grants.gov.

[71] For additional information on USDA's Rural Utility Service, refer to: http://www.rurdev.usda.gov/utilities_LP.html.

Funding and Sustainment Resources

OEC, SAFECOM, and NCSWIC publish numerous resources for state, local, tribal, and territorial governments and their public safety agencies to identify funding mechanisms for emergency communications projects. The following list includes educational documents and tools designed for stakeholders, available on the SAFECOM Funding website at: https://www.dhs.gov/safecom/funding.

- *Funding Mechanisms for Public Safety Communications Systems,* provides an overview of various methods of funding emergency communications systems (e.g., bonds, special tax, surcharges), and specific examples of where these methods have been used to fund state and local systems.
  - *Funding and Sustainment Methods for Public Safety Communications Systems* (2016 and 2015), present funding and sustainment methods used by state and local agencies to fund emergency communications systems.
- Various educational documents, brochures, and action memorandum to assist stakeholders identify funding and procure radio communications systems.
  - *LMR 101, Part I: Educating Decision Makers on LMR Technologies*, includes basic information for use in educating decision-makers about the importance of LMR technologies. The paper includes simple diagrams, terminology, history, and current usage of LMR technologies by public safety agencies.
  - *LMR for Decision Makers, Part II: Educating Decision Makers on LMR Technology Issues*, provides information about emerging technologies, and the impact such technologies will have on LMR systems as they evolve. Information includes discussion of the LMR-to-LTE transition, and the need to sustain mission critical voice through such transition.
  - *LMR for Project Managers, Part III: A P25 Primer for Project Managers and Acquisition Managers*, delivers an introduction about standards-based purchasing, and an overview of the P25 standard explaining its importance to public safety interoperability.
  - *LMR Brochure,* provides stakeholders with a hand-out to give to state and local decision-makers and elected officials to explain why it is important to fund and sustain LMR.
  - *LMR Action Memorandum,* provides stakeholders with basic information they can give to state and local decision-makers and elected officials on why it is important to fund and sustain public safety radio systems.
- *Emergency Communications System Life Cycle Planning Guide*, assists efforts to design, implement, support, and maintain a public safety communications system.
  - *Life Cycle Planning Tool*, provides additional information on funding considerations during each phase of the life cycle.
- *Interoperability Business Case: An Introduction to Ongoing Local Funding*, advises the community on the elements needed to build a strong business case for funding interoperable communications.

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
CAP	Common Alerting Protocol
CASM NextGen	Next Generation Communication Assets Survey and Mapping
CDM	Continuous Diagnostics and Mitigation
CFR	Code of Federal Regulations
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	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 Planning 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
GFIPM	Global Federated Identity and Privilege Management
GRA	Global Reference Architecture
HAVE	Hospital Availability Exchange
HF	High Frequency
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credentialing, and Access Management
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
NHTSA	National Highway Traffic Safety Administration
NIFOG	National Interoperability Field Operations Guide
NG911	Next Generation 911
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
NOFO	Notice of Funding Opportunity
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
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	State Interoperability Executive Committee
SLIGP	State and Local Implementation Grant Program
SMLA	Spectrum Management Lease Agreements
SOP	Standard Operating Procedure
SoR	Statement of Requirements
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
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

Grant recipients 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
  - FirstNet
  - 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)
- Alert and Warning Systems
  - 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, interoperability, and continuity remain top communications priorities.

To improve interoperability across investments, grantees are strongly encouraged to ensure 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.[72] Grant recipients should purchase P25 compliant systems and equipment that has been assessed as compliant in accordance with the P25 Compliance Assessment Program (CAP).[73] The P25 CAP is a partnership of the Department of Homeland Security (DHS) Office for Interoperability and Compatibility, industry, and the emergency response community. It is a formal, independent process for ensuring communications equipment declared by the supplier is P25 compliant and tested against the standards with publicly published results. The P25 CAP publishes Compliance Assessment Bulletins on policy, testing, and reporting requirements, as well as an approved equipment list that may be eligible for grant funds.

The P25 suite of standards is published by the Telecommunications Industry Association (TIA),[74] a recognized American National Standards Institute (ANSI) standards development organization. P25 standards provide many technical specifications for emergency communications equipment that are designed to ensure equipment is interoperable regardless of manufacturer. The P25 Steering Committee periodically publishes a list of "Approved Project 25 Suite of Standards" that includes the most recent documents and revisions.

The P25 Steering Committee, in coordination with the P25 User Needs Subcommittee, publishes the P25 Users Statement of Requirements (SoR) to address user needs on a periodic basis as new or revised requirements are identified. Although the SoR reflects 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 is strongly emphasized 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 published and accredited technical

[72] Applicants should read grant guidance carefully to ensure compliance with standards, allowable cost, documentation, reporting, and audit requirements.
[73] For information on the P25 CAP, see: https://www.dhs.gov/science-and-technology/p25-cap.
[74] 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.

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*[75] to determine which standards are applicable to the proposed purchase and project.
- Include all applicable P25 standards and expectations for interoperability in any Statement of Work (SoW) or acquisition documents for communications equipment 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.
- Obtain documented evidence of P25 compliance from the manufacturer that the equipment has been tested and passed all the applicable, published, normative P25 compliance assessment test procedures for performance, conformance, and interoperability as defined in the latest P25 Compliance Assessment Bulletins for testing requirements.[76] 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 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). 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 encrypted capabilities are compliant with the published P25 Block Encryption Protocol Standard. Grantees investing in encryption must 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.

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

[76] 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.

- Grantees seeking to use federal grant funds to purchase non-standard encryption features (e.g., 40-bit encryption, DES-OFB) or capabilities for new or existing equipment must ensure AES 256-bit is also included to ensure their devices have the capability to interoperate in an encrypted mode.
- 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.

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

P25 Resources

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

- LMR Trio: LMR 101, LMR for Decision Makers, and LMR for Project Managers: https://www.dhs.gov/safecom/funding
- PTIG: http://www.project25.org/ (Free registration required)
- P25 Suite of Standards: http://www.project25.org/images/stories/ptig/20160128_Approved_P25_TIA_Standards_Q1-2016.pdf
- P25 CAP: https://www.dhs.gov/science-and-technology/p25-cap
- P25 CAP Approved Equipment List: https://www.dhs.gov/science-and-technology/p25-cap-grant-eligible-equipment
- P25 Compliance Assessment Bulletins: https://www.dhs.gov/science-and-technology/p25-cap
- Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems: https://www.dhs.gov/sites/default/files/publications/20160830%20Best%20Practices%20for%20Encryption_Final%20Draft508.pdf

- Guidelines for Encryption in Land Mobile Radio Systems: https://www.dhs.gov/sites/default/files/publications/20160204_Guidelines%20for%20Encryption%20in%20Land%20Mobile%20Radio%20Systems_Final508c_0_0.pdf
- Considerations for Encryption in Public Safety Radio Systems: https://www.dhs.gov/sites/default/files/publications/20160830%20Considerations%20for%20Encryption_Final%20Draft508_0.pdf

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 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.

The Middle Class Tax Relief and Job Creation Act of 2012 authorized $115 million for a targeted 911 Grant Program administered by the Department of Transportation National Highway Traffic Safety Administration and the Department of Commerce National Telecommunications and Information Administration (NTIA). Recipients should visit https://www.911.gov/project_911grantprogram.html for additional information and to sign up to receive email updates as new information is available. Other federal programs include 911 projects as an eligible use of funds. For a full list of federal grant and loan programs that allow 911 activities, visit: https://www.911.gov/federal_grants_opportunities.html.

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 solutions developed or procured meet industry guidelines and standards.

Grantees and the 911 community are encouraged to consider the following options[77] 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[78]
- 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 to facilitate the ongoing coordination required to plan, deploy, operate, and maintain NG911 systems
- Develop contract language to ensure 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: http://www.911.gov/
- *NG911 Standards Identification and Review*: https://www.911.gov/pdf/National_911_Program_NG911_Standards_Identification_Analysis_2016.pdf
- Benefits of NG911: A Video: https://www.911.gov/ng911movie.html
- "State of 911" Webinars: https://www.911.gov/webinars.html
- NG911 for Leaders in Law Enforcement: https://www.911.gov/nglawenforcement.html
- Nationwide 911 statistics: https://www.911.gov/issue_911statsanddata.html
- 911 Legislation Tracking & Models: https://www.911.gov/project_911nationallegislationtracking.html
- Recommended Minimum Training for 911 Telecommunicators: https://www.911.gov/project_recommended911minimumtrainingfortelecommunicators.html
- Federal Funding Programs for 911: https://www.911.gov/federal_grants_opportunities.html
- The 911 Interstate Playbook: https://www.911.gov/project_nextgeneration911interstateplaybook.html
- NG911 Procurement Guidance: https://www.911.gov/pdf/National_911_Program_NG911_Procurement_Guidance_2016.pdf

[77] 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.

[78] 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.

- *NG911 and FirstNet: A Guide for State and Local Authorities*: https://www.911.gov/pdf/NASNA_National_911_Program_NG911_FirstNet_Guide_State_Local_Authorities.pdf

National Association of State 911 Administrators

The National Association of State 911 Administrators (NASNA) facilitates coordination and information sharing between State programs that operate 911 systems. Additional 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, has developed a series of 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, including an NG911 Readiness Checklist and specific information on 911 cybersecurity and funding, 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.

NG911 Institute

The NG911 Institute has members throughout the Nation who are dedicated to advancing NG911 services. Members include public safety officials, telecommunication and industry professionals, policy makers, academia, and concerned citizens. The mission of the NG911 Institute is to assist the Congressional NextGen 911 Caucus by serving as a broad educational resource on issues important to the effective operation and advancement of NG911 services and systems. The overarching objective of the NG911 Institute is to advance the rapid implementation of NG911 to promote more effective emergency response, improve public safety, and advance national security interests. More information is available at: http://www.ng911institute.org/.

NG911 NOW Coalition

The NG911 NOW Coalition is comprised of national public safety leaders and industry, which have joined together to create a coalition focused on rapidly accelerating the deployment of NG911. Coalition members are working to address the funding, technical, policy, and legislative challenges that have stalled more rapid NG911 implementation. The NG911 NOW Coalition aims to, by 2020, have all 911 systems and centers in all 56 states and territories have sufficiently funded, standards-based, end-to-end, IP-based capabilities, and will have retired legacy 911 systems, without any degradation to the public. More information is available at: http://www.ng911now.org/.

Public Safety Broadband

FirstNet

The First Responder Network Authority's (FirstNet) mission is to deploy, operate, and maintain the Nationwide Public Safety Broadband Network (NPSBN)[79] to provide Long-Term Evolution (LTE)-based broadband services and applications to public safety entities.[80] The network is a single, nationwide network architecture consisting of a core network, transport backhaul, and radio access network (RAN). While mission critical voice communications will continue to occur on LMR, in time, FirstNet is expected to provide the public safety community with mission critical broadband data capabilities and services including, but not limited to:

- Messaging
- Image Sharing
- Video Streaming
- Group Text
- Voice
- Data Storage
- Applications
- Location-based Services
- Quality of Service, Priority and Preemption

[79] The Middle Class Tax Relief and Job Creation Act of 2012 (P.L. 112-96) authorized establishment of the NPSBN.
[80] 47 U.S.C. § 1401(26) (defining the term public safety entities).

FirstNet is responsible for developing the network architecture, technical and user requirements, spectrum access policies, standards, and deployment plans for the network. As the NPSBN is deployed, FirstNet will continue to actively engage public safety entities, federal, state, local, tribal, and territory jurisdictions, and other stakeholders.

FirstNet submitted a detailed State Plan to each state and territory describing how FirstNet intends to deploy the network in that state or territory. Governors were to then decide whether to adopt the FirstNet State Plan (and thus have the network deployed in their state at no cost) or whether they wish to take on the full risk and responsibility of developing an alternative State Plan. All 50 States, 5 Territories, and the District of Columbia adopted the FirstNet State Plan and network deployment is ongoing.

While entities may want to pursue funding for broadband equipment and systems on commercially designated spectrum, there are no assurances that such equipment and systems will be compatible with FirstNet. Therefore, FirstNet strongly advises grantees to coordinate with FirstNet in advance of any strategic acquisition of LTE equipment to ensure purchases support future service choices. Grantees are encouraged to further focus on planning and outreach activities (e.g., community outreach and education, documenting user needs) and to work with any applicable governing bodies in planning for the arrival of broadband and other advanced technologies.[81] This includes:

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

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 any applicable governing bodies and

[81] 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.

FirstNet to ensure the project does not conflict with network deployment efforts and that the project complies with all 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.[82]

However, given ongoing advancements in FirstNet's deployment and interoperability challenges of various technologies, grantees should consider the overall impact of using other wireless broadband technologies at this time. Before the Technical Advisory Board for First Responder Interoperability developed recommended minimum technical requirements for the network based on commercial standards for LTE service, public safety agencies considered other wireless broadband technologies such as WiMAX.[83] LTE was endorsed by public safety organizations for economies of scale, radio frequency use, and spectral efficiency reasons.[84] Moreover, major wireless service providers chose LTE for their broadband data services and in 2010, the FCC designated LTE as the required technology for FirstNet.[85] Thus, grantees are strongly encouraged to focus on preparation for the network and working with FirstNet and any applicable governing bodies 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 communications capabilities and help the agencies plan for and prepare for the deployment of the network.

Public Safety Broadband Resources

- FirstNet: https://www.firstnet.gov/ or https://www.firstnet.com/
- NTIA BroadbandUSA Program: https://www2.ntia.doc.gov/
- NTIA State and Local Implementation Grant Program (SLIGP) 2.0: https://www.ntia.doc.gov/sligp2/program-information
- Public Safety Communications Research (PSCR) Program: https://www.nist.gov/ctl/pscr/public-safety

---

[82] FCC Tech Topic #11: WiMAX Applications for Public Safety at: http://transition.fcc.gov/pshs/techtopics/techtopics11.html.
[83] See 47 U.S.C. § 1423 (a), (c)(1). Technical Advisory Board for First Responder Interoperability at: https://www.fcc.gov/general/technical-advisory-board-first-responder-interoperability.
[84] See: http://www.npstc.org/documents/Press_Release_NPSTC_Endorses_LTE_Standard_090610.pdf.
[85] FCC, 700 MHz Public Safety Spectrum: http://www.fcc.gov/encyclopedia/700-mhz-spectrum.

Data Information Sharing Systems

Data information sharing systems are becoming more prevalent within the emergency communications community. Information sharing solutions are as fundamental as a digital data "snapshot" transferred over electronic media, or as tailored as custom-interface applications that allow proprietary applications to be linked. Challenges for effective information exchange include increasing types of data being exchanged, such as video, geographic information system (GIS) data, evacuee/patient tracking data, accident/crash (telematics) data, biometric data, Computer-Aided Dispatch (CAD) data, Automatic Vehicle Location (AVL) data, Common Operation Picture data, and more.[86]

To communicate seamlessly with the increasingly interconnected systems of the broader community, grantees should consider standards-based information exchange models. A few of widely used exchange models are provided as part of this appendix; however, an evaluation of who the organization most often communicates with, and what types of information are commonly exchanged, is recommended in selecting an ideal data information sharing solution.

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

The OASIS EDXL suite of data messaging standards facilitate information sharing among public safety agencies. Grant-funded systems, developmental activities, or services related to emergency response information sharing should comply with OASIS EDXL suite of data messaging standards. Compliance should include the following OASIS EDXL standards:

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

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, or visit their Emergency Management Technical Committee's site (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency), which includes EDXL overview videos.

[86] For any grant funding software-based patient tracking products, the product is strongly encouraged to comply with the following Oasis and HL-7 standards: "OASIS EDXL-TEP" and Bi-directional Transformation of OASIS EDXL-TEP (Tracking of Emergency Patients) v1.1 and HL7 v2.7.1 Specification Version.

National Information Exchange Model (NIEM)

NIEM is a framework established by 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 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.[87]

Global Reference Architecture (GRA)

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

Many Department of Justice grant solicitations require its grantees to comply with the GRA—specifically the Global Standards Package—which describes a full information sharing

[87] Applicants 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 grant recipients which can be found at: https://www.niem.gov/aboutniem/grant-funding/Pages/implementation-guide.aspx.

technology standards implementation suite that addresses data standardization, messaging architecture, security, and privacy requirements. For additional information on GRA, including technical assistance and training opportunities, visit the Office of Justice Programs website at: https://it.ojp.gov/initiatives/gra.

Alert and Warning Systems

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 allows authorities to deliver alerts simultaneously through multiple communications pathways 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. WEA is especially beneficial as it allows for geographically targeted alerts via wireless cell broadcasts, even when cellular networks are congested.

Standards for IPAWS

In order to access IPAWS, grantees should select equipment and applications that adhere to both CAP and IPAWS Profile standards. The CAP standard is an open, non-proprietary digital format for exchanging emergency alerts that was developed by OASIS.[88] CAP allows a consistent alert message to be disseminated simultaneously over many different dissemination mechanisms. The CAP format is compatible with emerging technologies, such as web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' NOAA Weather Radio and the EAS, while offering enhanced capabilities including images, maps, and video.

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 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, piece of software, or equipment. Test results for any alert and warning software or equipment tested at the IPAWS Lab can be made available to assist 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-

[88] Latest CAP version available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#tc-tools.

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, exercising, replacement, and maintenance of alert and warning systems, software, and equipment.

Alerts and Warning Resources

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

LMR has long been used by emergency first responders for mission critical communications. As technologies evolve, LMR systems are exposed to greater security risks such as jamming, eavesdropping, and denial of service. In addition, the emergency response community is deploying advanced voice, video, and data services over 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. According to the U.S. Computer Emergency Readiness Team (US-CERT), from 2014 through 2016, federal agencies reported more than 177,000 cybersecurity incidents, with more than 50,000 involving personally identifiable information.[89] State, local, tribal, and territorial governments, and commercial entities have also experienced a significant increase in attacks and emergency communications is a common target. 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. While not an exhaustive list as cyber threats continue to change, grantees should be aware of the risks to their systems.

[89] Latest Government Accountability Office report available at: https://www.gao.gov/assets/700/690081.pdf.

Table B-1. Example Cyber Risks to Emergency Communications Systems

Components	Cyber Risks
Devices and Equipment	• **Data breaches:** Data stored 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 solutions.[90] 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 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.

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. 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.[91] Recipients are strongly encouraged to implement NIST's framework to complement an existing risk management process or to develop a credible program if one does not exist. The Critical Infrastructure Cyber Community C³ Voluntary Program supports owners and operators of critical infrastructure, academia, Federal Government, state, local, tribal, and territorial governments, and businesses in their use of the NIST Cybersecurity Framework.[92]

[90] 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."
[91] NIST *Framework for Improving Critical Infrastructure Cybersecurity* is available at: https://www.nist.gov/cyberframework.
[92] Critical Infrastructure Cyber Community C³ Voluntary Program: http://www.dhs.gov/ccubedvp.

The NIST Cybersecurity Framework establishes five functions to integrate cybersecurity into mission functions and operations, including: 1) ***identify***, evaluate, and prioritize risks for their entity; 2) ***protect*** against identified risks; 3) ***detect*** risks to the network as they arise; 4) deploy ***response*** capabilities to mitigate risks; and 5) establish ***recovery*** protocols to ensure the resiliency and continuity of communications. DHS's Emergency Services Sector has developed tailored guidance specific to emergency service disciplines, including a NIST Framework implementation guide with a repeatable process to identify and prioritize cybersecurity improvements.[93] Table B-2 highlights some fundamental cybersecurity best practices for recipients to reference in the development of a more tailored and comprehensive cybersecurity strategy.

Table B-2. Cybersecurity Best Practices

Function	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 each 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, whether in transit or at rest • **Security Policies.** Establish, enforce, and update consistent security policies as new threats emerge • **Training.** Develop role-specific training for users and administrators on security, resiliency, and operations

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

Function	Best Practices
Detect	• **Continuous Monitoring.** Develop or use existing government continuous monitoring diagnostics and mitigation capabilities, such as DHS' Continuous Diagnostics and Mitigation (CDM) Program[94] • **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 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 or use 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.** Establish and maintain redundancy, route diversity, and policies/procedures to promote network reliability, resiliency, and continuity of service • **Coordination.** Coordinate restoration activities with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, response partners, and vendors • **Process Improvements.** Improve recovery planning processes and strategies by incorporating lessons learned into future activities. Train response personnel on the latest security, resiliency, continuity and operational practices and maintain in-service training as new technology and methods are made available

Standards for Cybersecurity

There is considerable cybersecurity guidance available from government, industry, and academic organizations and a multitude of 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

Standards Originations	Standards
American National Standards Institute (ANSI) / International Society of Automation (ISA)	ANSI/ISA standards focus on automation and control systems solutions. The NIST Cybersecurity Framework recommends two ANSI/ISA standards for use: ANSI/ISA-62443-2-1 (99.02.01)-2009 and ANSI/ISA-62443-3-3 (99.03.03)-2013. https://www.isa.org/templates/two-column.aspx?pageid=131422. Also, outputs of the ATIS Emergency Services Interconnection Forum, Next Generation Interconnection Interoperability Forum, and Wireless Technologies and Systems Committee are important to the public safety community.

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

Standards Originations	Standards
Criminal Justice Information Services (CJIS) Security Policy	CJIS standards contain information security requirements, guidelines, and agreements reflecting the will of law enforcement agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information. https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center
European Telecommunications Standards Institute (ETSI)	ETSI Telecommunications & Internet converged Services & Protocols for Advanced Networks (TISPAN) has been a key standardization body in creating Next Generation Network (NGN) specifications, and their Cyber Security committee focuses entirely on privacy and security activities. Of note for emergency communications are the ETSI TS 102, 123, 182, and 282 series. http://www.etsi.org/
Federal Information Processing Standards (FIPS)	FIPS establishes the minimum security requirements for federal information systems. https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Legislation enacted by Congress in 1997 to streamline medical regulations, privacy considerations, and the efficiency and security of medical care. The standards/rules associated with HIPAA address some of the NIST Cybersecurity Framework functions. https://www.hhs.gov/hipaa/
IEEE	IEEE produces sector-specific security standards, as well as industry guidance. Of interest to networks may be the 802, 1363, and 1619 series, as well as C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. http://www.ieee.org/
International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Standards	The ISO/IEC 27000 series of standards provide a foundation for information security management best practices. Of interest to emergency communication networks may be ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27002, ISO/IEC 27032, and ISO/IEC 17799. http://www.iso.org
International Telecommunication Union (ITU)	A fundamental role of ITU is to build confidence and security in the use of Information and Communication Technologies. Of note for emergency communications networks include X.800, X.805, and X.1051. http://www.itu.int/
Internet Engineering Task Force (IETF)	IETF Working Groups are the primary mechanism for development of IETF standards. IETF Working Groups currently have 598 standards regarding security mechanisms, integrity mechanisms, network layer security, transport layer security, application layer security, encryption algorithms, key management, secure messaging, etc. https://www.ietf.org/
National Emergency Number Association (NENA) Security for Next Generation 911 (NG911) Standard (NG-SEC)	Of note for NG911 networks include NENA-STA-010, Detailed Functional and Interface Specification for the NENA i3 Solution; NENA 75-001: NENA Security for Next Generation 911 Standard (NG-SEC); NENA 75-502: NG-SEC Audit Checklist; NENA 04-503: Network/System Access Security Information Document, and NENA-INF-015.1-2016: NG911 Security Information Document. http://www.nena.org/
National Fire Protection Association 1221	A standard for the installation, maintenance, and use of emergency services communications systems, including cybersecurity considerations. http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1221
NG911 Program Standards Identification and Review	These standards collected from all major standards bodies and address cybersecurity when planning for NG911 deployments. https://www.911.gov/documents_tools.html. Documentation under the "Cybersecurity" tab is also of use.

Standards Originations	Standards
NIST Recommendations on Cybersecurity (Special Publications 800 Series)	NIST's 800 series provides targeted cybersecurity guidance and are strongly encouraged to be incorporated into cybersecurity planning. http://csrc.nist.gov/publications/PubsSPs.html
North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Regulations	Reliability standards address the security of cyber assets essential to the reliable operation of the electric grid. With emerging interconnectivity of infrastructure, the emergency communications community may also need to address these standards. http://www.nerc.com/pa/CI/Comp/Pages/default.aspx
Organization for the Advancement of Structured Information Standards (OASIS)	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). https://www.oasis-open.org/
Telecommunications Industry Association (TIA)	TIA has both Cybersecurity and Public Safety working groups. Standards of particular use for emergency communications include: TR-8, TR-30, TR-34, TR-41 TR-42 TR-45, TR-47, TR-48, TR-49, TR-50 M2M, TR-51, and TIA-102. https://www.tiaonline.org/
Third Generation Partnership Project (3GPP) Security Standards	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. www.3gpp.org
World Wide Web Consortium (W3C)	Includes web cryptography, web application security, web payments, and XML security. https://www.w3.org/

Cybersecurity Resources

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

Committee on National Security Systems (CNSS) Guidance

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

DHS

- C³ Voluntary Program Cyber Resilience Review (CRR): https://www.us-cert.gov/ccubedvp/assessments
- Communications Sector-Specific Plan (CSSP): An Annex to the National Infrastructure Protection Plan: https://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf
- Continuous Diagnostics and Mitigation (CDM): http://www.gsa.gov/portal/content/177895
- Cybersecurity Evaluation Tool (CSET): https://ics-cert.us-cert.gov/Assessments
- Emergency Services Sector (ESS) Cyber Risk Assessment – 2012: http://www.dhs.gov/publication/emergency-services-sector-cybersecurity-initiative

- ESS Roadmap to Secure Voice and Data Systems – 2014: https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Roadmap-to-Secure-Voice-and-Data Systems-508.pdf
- ESS Cybersecurity Framework Implementation Guidance – 2015: https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/ess-framework-implementation-guide-2015-508.pdf
- Emergency Services Sector-Specific Tabletop Exercise Program (ES SSTEP): https://www.dhs.gov/publication/es-sstep-fact-sheet
- 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
- Information Sharing Environment (ISE) Guides and Best Practices: https://www.ise.gov/resources/standards-guides-best-practices
- National Cyber Incident Response Plan: https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
- 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
- Guidelines for Encryption in Land Mobile Radio Systems: https://www.dhs.gov/sites/default/files/publications/20160204_Guidelines%20for%20Encryption%20in%20Land%20Mobile%20Radio%20Systems_Final508c_0.pdf
- Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems: https://www.dhs.gov/sites/default/files/publications/20160830%20Best%20Practices%20for%20Encryption_Final%20Draft508.pdf

Energy

- Energy Sector Cybersecurity Capability Maturity Model (C2M2) Program: http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

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
- EO 13407: Public Alert and Warning System: https://www.gpo.gov/fdsys/pkg/WCPD-2006-07-03/pdf/WCPD-2006-07-03-Pg1226.pdf

Federal Bureau of Investigation

- Internet Crime Complaint Center: www.IC3.gov

FCC

- Communications Security, Reliability and Interoperability Council (CSRIC): https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability
- Task Force on Optimal PSAP Architecture (TFOPA): https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point
- Cyber Security Planning Guide: http://transition.fcc.gov/cyber/cyberplanner.pdf

FEMA

- Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC): https://www.usfa.fema.gov/operations/ops_cip_emr-isac.html

GAO

- U.S. Government Accountability Office, Cybersecurity: https://www.gao.gov/key_issues/overview

NIST

- Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/
- Internal/Interagency Reports (NISTIR): http://csrc.nist.gov/publications/PubsNISTIRs.html
- National Initiative For Cybersecurity Education (NICE): https://www.nist.gov/itl/applied-cybersecurity/nice
- NICE Cybersecurity Workforce Framework: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Industry and Associations

- ATIS Industry Best Practices: http://www.atis.org/bestpractices/Search.aspx

- APCO: https://www.apcointl.org/, specifically APCO Cybersecurity Guide for Public Safety Community Professionals and APCO Introductory Guide to Cybersecurity for PSAPs ISACA COBIT 5 Framework: https://cobitonline.isaca.org/
- 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
- NASCIO Cybersecurity Awareness: https://www.nascio.org/Advocacy/Cybersecurity, including NASCIO Cyber Disruption Response Planning Guide for States
- National Conference of State Legislation Cybersecurity Training for State Employees: http://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx
- OWASP Top Ten Project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- OWASP Internet of Things Project: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Appendix C – Emergency Communications Resources

This appendix provides links to resources referenced in the *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 DHS/FEMA's AEL at: http://www.fema.gov/authorized-equipment-list
- Project 25 Compliance Assessment Program list of approved radio equipment: https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment

Broadband
- First Responders Network Authority (FirstNet) Website: http://www.firstnet.gov
- 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: http://www2.ntia.doc.gov/
- Broadband Initiatives Program: http://www.rd.usda.gov/recovery/broadband.html
- U.S. Department of Agriculture Rural Utilities Farm Bill Broadband Loan Program: http://www.rurdev.usda.gov/RUSTelecomPrograms.html
- Interoperability Planning for Wireless Broadband: http://www.dhs.gov/safecom/resources-library
- 3GPP RAN5 Mobile Terminal Conformance Testing: http://www.3gpp.org/specifications-groups/ran-plenary/ran5-mobile-terminal-conformance-testing

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*
- OASIS: 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 DHS/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: https://www.dhs.gov/safecom/resources-library
- Exercises conducted for DHS/FEMA preparedness grants must be National Incident Management System compliant: http://www.fema.gov/national-incident-management-system
- NIMS National Standard Curriculum Training Development Guidance: https://www.fema.gov/training-0

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
- FEMA Grants: https://www.fema.gov/grants
- FEMA Information Bulletins: https://www.fema.gov/grants/grant-programs-directorate-information-bulletins

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

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

Grants Listings
- List of grants funding emergency communications: https://www.dhs.gov/safecom/funding

- Grants.gov Website: https://www.grants.gov
- FEMA Grants Website: https://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

Land Mobile Radio (LMR)
- LMR Trio – LMR 101, LMR for Decision Makers, and LMR for Project Managers: https://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: https://www.dhs.gov/safecom/resources-library

Middle Class Tax Relief and Job Creation Act
- To obtain a copy of the Act, see: http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf

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)
- https://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)
- https://www.dhs.gov/national-interoperability-field-operations-guide-nifog

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://www.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/
- Federal Funding Programs for 911: https://www.911.gov/911grants.html
- NG911 Standards Identification and Review: https://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
- 911 Interstate Playbook: https://www.911.gov/docs/NG911-Interstate-Playbook-FINAL-111516.pdf
- NG911 Procurement Guidance: https://www.911.gov/docs/N9P-NG911-Procurement-Guidance-Final-Oct-2016.pdf
- NG911 NOW Coalition: http://www.ng911now.org/

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

Office of Emergency Communications (OEC)
- Website: https://www.dhs.gov/office-emergency-communications
- Contact Information: oec@hq.dhs.gov
- Guidance Documents: https://www.dhs.gov/safecom/resources-library
- 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
- http://www.whitehouse.gov/omb/grants_default/

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
- Government Emergency Telecommunications Service: http://www.dhs.gov/gets
- Wireless Priority Service: http://www.dhs.gov/wps
- Telecommunications Service Priority: http://www.dhs.gov/tsp

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): https://www.dhs.gov/science-and-technology/p25-cap

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

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

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/resources-library

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 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

Appendix D – Compliance Requirements for DHS Grants

This appendix provides guidance for Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) preparedness 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*. DHS/FEMA recipients should also refer to the specific Notice of Funding Opportunity for all programmatic requirements that apply (https://www.fema.gov/preparedness-non-disaster-grants).

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

Topics	Requirements
National and Statewide Plan Alignment Sections 2.2, 2.5, 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, 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 body and leadership. • Explain how proposed projects address or support communications resiliency.
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 the NECP. • 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. • Designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government, to include establishing statewide plans, policies, and procedures, and coordinating decisions on communications investments funded through federal grants. • Coordinate proposals with statewide emergency communications governance bodies and leaders (e.g., State Interoperability Executive Committee, SWIC, 911 Administrator).
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 https://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. Recipients 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.

Topics	Requirements
Spectrum Licensing Section 3.3	• If project requires new spectrum license, consult the appropriate statewide coordinator (e.g., SWIC), the Federal Communications Commission, and/or FirstNet to ensure the recipient 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 (as directed above) and Threat and Hazard Identification and Risk Assessment (THIRA). The Comprehensive Preparedness Guide 201 provides a four-step process for conducting a THIRA. Follow THIRA submission instructions in program guidance.
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 https://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. Recipients 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 DHS/FEMA programs, and the P25 Compliance Assessment Program Approved Equipment List. If proposal includes any non-P25 LMR equipment, recipients must apply for prior approval.
Next Generation 911 (NG911) Systems Sections 2.5, 4.5, 5, Appendix B	• 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	• Consult with applicable governing bodies and leaders for the latest guidance from FirstNet, planning for public safety broadband network activities, and identifying the authority to operate on public safety spectrum. For additional information, refer to https://www.firstnet.gov/.
Alerts and Warnings Sections 2.5, 4.5, 5, Appendix B	• 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.