SAFECOM Guidance on Emergency Communications Grants

Fiscal Year 2025

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

A Message to Stakeholders

On behalf of the Cybersecurity and Infrastructure Security Agency (CISA), I am releasing the *Fiscal Year 2025 SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)*. This document is updated annually to provide current information on emergency communications policies, best practices, and technical standards for state, local, tribal, and territorial grant applicants and recipients investing Department of Homeland Security grant funds in emergency communications projects.

This *SAFECOM Guidance* aligns with the *National Emergency Communications Plan* (NECP), which emphasizes the need to enhance governance structures, plans, and protocols that enable the emergency response community to communicate requisite information under all circumstances. Grant applicants are encouraged to support the guidelines within the NECP to maximize the use of voice, video, and data communications and to ensure the security of data and information exchange. The *SAFECOM Guidance* also addresses the rapidly evolving emergency communications ecosystem. Over the past few years, the emergency communications community has been greatly affected by increasing cyber-attacks on critical infrastructure and systems. Recognizing these challenges, CISA strongly encourages applicants to review the best practices and resources available in the *SAFECOM Guidance* to help navigate this shifting landscape.

The SAFECOM Guidance is broadly accepted as the primary guidance on emergency communications grants. Since 2015, the Department of Homeland Security has required its grant recipients investing in emergency communications using federal dollars to comply with *SAFECOM Guidance*. All grant applicants are encouraged to coordinate with their statewide governance bodies and emergency communications leaders (e.g., Statewide Interoperability Coordinators) to ensure projects support the state, local, tribal, or territory's strategy to improve interoperable emergency communications. In addition, grant applicants 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 grant applicants to participate, support, and invest in planning activities that will help states, locals, tribes, and territories prepare for deployment of new emergency communications systems or technologies. Grant applicants should continue enhancing governance and leadership, developing plans and procedures, conducting training and exercises, and investing in standards-based equipment to sustain land mobile radio capabilities, while concurrently planning for the integration and deployment of new voice, data, and video communications technologies. Grant applicants must also consider cybersecurity risks across all capabilities when planning operable, interoperable, and continuity of communications.

As in previous years, CISA developed the *SAFECOM Guidance* in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators. CISA also consulted federal partners and the Emergency Communications Preparedness Center to ensure emergency communications policies are coordinated and consistent across the federal government. Grant applicants for Department of Homeland Security grants are encouraged to reference this document when developing emergency communications investments for federal funding, and to direct any questions to ECD@cisa.dhs.gov.

Billy Bob Brown, Jr
Executive Assistant Director for Emergency Communications
Cybersecurity and Infrastructure Security Agency

Contents

1. Introduction

The Department of Homeland Security (DHS) is mandated by the Homeland Security Act to administer responsibilities and authorities relating to the SAFECOM Program.[1] Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for developing coordinated guidance for federal grant programs for public safety communications.[2] As a result, CISA 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 the *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 *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 recommends policies and standards across federal grant programs to provide a consistent approach to improving emergency communications nationwide. The *SAFECOM Guidance* achieves this consistency by aligning recommendations with the *National Emergency Communications Plan* (NECP).[4]

SAFECOM is a public safety stakeholder-driven program sponsored by CISA, which develops policy, guidance, and future efforts by drawing on SAFECOM member expertise and recommendations. The DHS Science and Technology Directorate 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 communications.

Additionally, CISA consulted members of the Emergency Communications Preparedness Center (ECPC), which coordinates roles and activities of agencies across the federal government to improve interoperable public safety and emergency response communications. ECPC consists of 14 federal departments and agencies representing the government's broad role in improving coordination of emergency communications efforts, including information sharing, planning, regulation, policy, operations, grants, and technical assistance. Together, SAFECOM members and federal partners coordinate 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 insight to grant applicants and recipients[5] about:

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

[1] *See* 6 U.S.C. § 571(c)(2); For more information on SAFECOM, see: cisa.gov/safecom.
[2] 6 U.S.C. § 574.
[3] Federal financial assistance includes grants, loans, cooperative agreements, and other funds provided by the federal government. For this document, these terms are used interchangeably unless otherwise indicated.
[4] The NECP is the nation's strategic plan for emergency communications and is available at: cisa.gov/national-emergency-communications-plan.
[5] In accordance with Title 2 of the Code of Federal Regulations (CFR) 200, the terms "recipient" and "sub-recipient" are defined as non-federal entities that receive federal awards 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 vision established in the NECP. CISA published a second update to the NECP in September 2019 that builds upon revisions made in 2014, while also positioning the NECP to maintain its relevance in the future. Updates to the NECP goals and objectives 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 plan's success relies on the whole community embracing the NECP goals and objectives, and most importantly implementing them. Critical components for advancing emergency communications fall under three national priorities:

- Enhance effective governance across partners with a stake in emergency communications, embracing a shared responsibility of the whole community from traditional emergency responders and supporting entities to the citizens served
- Address interoperability challenges posed by rapid technological advancements and increased information sharing, ensuring the most critical information gets to the right people at the right time
- Build resilient and secure emergency communications systems to reduce cybersecurity threats and vulnerabilities

Recommendations within the *SAFECOM Guidance* are intended to help state, local, tribal, and territorial stakeholders develop projects that meet critical emergency communications needs as defined in the NECP and their Statewide Communication Interoperability Plan (SCIP).[6] Best practices and technical standards located within the *SAFECOM Guidance* help ensure federally funded investments are interoperable, fully effective and reliable, and support national policies. However, not all guidance is applicable to all grant programs. Grants funding emergency communications are administered by numerous federal agencies and are subject to various legal 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 Methodology

CISA consults with federal, state, local, tribal, and territorial partners to develop the *SAFECOM Guidance*, including:

- ECPC Grants Focus Group[8]
- Federal Communications Commission (FCC), Public Safety and Homeland Security Bureau (PSHSB)
- SAFECOM[9] and the National Council of Statewide Interoperability Coordinators (NCSWIC)
- U.S. Department of Commerce
  - First Responder Network Authority (FirstNet Authority)
  - National Institute of Standards and Technology (NIST)
  - National Telecommunications and Information Administration (NTIA)
- U.S. Department of Homeland Security
  - Federal Emergency Management Agency (FEMA) Grant Programs Directorate and the Integrated Public Alert and Warning System (IPAWS) Program Management Office
  - Science and Technology Directorate, Office for Interoperability and Compatibility
- U.S. Department of Justice, Office of Justice Programs
- U.S. Department of Transportation, National Highway Traffic Safety Administration (NHTSA)

[6] For information on SCIPs, see: cisa.gov/statewide-communication-interoperability-plans.
[7] For the purposes of this document, "grant guidance" may include Notices of Funding Opportunity, Grant Notices, and other formal notices of grants and federal financial assistance programs.
[8] 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.
[9] For a list of SAFECOM members, see: cisa.gov/safecom/membership.

1.3 Use of SAFECOM Guidance

The *SAFECOM Guidance* should be used during the planning, development, and implementation of emergency communications projects and in conjunction with other planning documents. Before proposing projects for funding, prospective applicants are encouraged to read the NECP, federal and state-specific preparedness documents (e.g., statewide plans and reports), and this *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 applicants.

Table 1. Essential Resources for Emergency Communications Grant Applicants

Resources	Descriptions
National Emergency Communications Plan	The NECP is the nation's strategic plan to strengthen and enhance emergency communications capabilities. It provides guidance to those that plan for, coordinate, maintain, invest in, and use communications to support response and recovery operations. Grant applicants are encouraged to read the NECP to understand the national strategy, and to ensure investments support the goals and objectives.
Statewide Communication Interoperability Plan	The SCIP contains the state, territory, or tribal government's strategy to improve emergency communications. States and territories were required to develop and submit a SCIP to DHS by December 2008 and required to submit reports annually on the progress of the state or territory in implementing its SCIP. Many federal grants funding emergency communications require grant applicants to align projects to needs identified in SCIPs. Grant applicants should review the SCIP for their state/territory and work with their Statewide Interoperability Coordinator (SWIC) to ensure investments support statewide plans to improve communications. Contact your SWIC to find your state or territory's SCIP.
SAFECOM Website	This website provides information and resources for public safety agencies developing emergency communications projects. Visit this website for the most recent *SAFECOM Guidance* and list of grants funding emergency communications.
IPAWS Website	This website contains information on IPAWS capabilities, who can use IPAWS to send alerts, warnings, and notifications (AWN), how agencies can become Alerting Authorities, and the availability of IPAWS Technical Support Services. IPAWS is accessed through IPAWS-compatible software with the capability to draft an AWN in Common Alerting Protocol format, a requirement of IPAWS Open Platform for Emergency Networks. While there is no cost to send messages through IPAWS, there are costs associated with acquiring IPAWS-compatible alert origination software. Grant applicants 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 AWN.
FirstNet Website	Grant applicants interested in investing federal funds in broadband-related projects potentially using the Nationwide Public Safety Broadband Network (NPSBN), also known as FirstNet, should consult with the First Responder Network Authority (FirstNet Authority), within the U.S. Department of Commerce, and the federal granting agency to understand all requirements impacting broadband investments. Contact your state or territory's FirstNet Authority advisor for information.
National Incident Management System (NIMS) Website	NIMS guides all levels of government, nongovernmental organizations, and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. FEMA offers training, guidance, and tools for NIMS implementation.

Resources	Descriptions
Office of Management and Budget (OMB) Circulars	Federal awards must adhere to the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* regulations, available on the Electronic Code of Federal Regulations website. Applicants for DHS grant programs should reference specific Notices of Funding Opportunity to determine applicable requirements at Grants.gov. Additional information is on the Chief Financial Officers Council website.
Statewide Interoperability Coordinator	States and territories 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. DHS/FEMA requires all states and territories that use 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. Contact information for SWICs can be found on the NCSWIC membership page.
State Leadership	States and territories have designated leadership positions to assist with emergency communications projects and may include an individual or body. These leadership positions vary by area and may have resulted from grant program requirements to designate a single point of contact, such as a **Broadband Coordinator**.
	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 (CIO), Chief Technology Officer, and Chief Information Security Officer (CISO) 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. Grant applicants are encouraged to coordinate 911 projects with the administrator to ensure projects support state or territory 911 efforts. To find your administrator, refer to the National Association of State 911 Administrators website.
	Consistent with each state's authorities, 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 the State Homeland Security and Emergency Services website.
State Governance	The **Statewide Interoperability Governing Body (SIGB)** or **State Interoperability Executive Committee (SIEC)** serves as the primary steering group for the statewide interoperability strategy that seeks to improve emergency response communications across the state through enhanced data and voice communications interoperability. SIGBs and SIECs include representatives from various jurisdictions and disciplines, as well as subject matter experts. Contact CISA to find the SIGB or SIEC for your state or territory.
	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. Grant applicants are encouraged to coordinate 911 projects with the appropriate board to ensure projects support broader state or territory 911 efforts. To find your 911 Advisory Board, refer to State 911 Contacts page.

2. Emergency Communications Priorities

CISA is responsible for ensuring grant guidelines and priorities relating to interoperable emergency communications are coordinated and consistent with the NECP goals and recommendations. In support of this mandate, *SAFECOM Guidance* identifies six investment priorities of equal merit. These priorities were developed in coordination with stakeholders and federal partners, and are informed by the NECP, as well as other applicable Presidential Policy Directives, federal statutes, and regulations. Grant applicants are encouraged to target grant funding toward the following priorities:

- Governance and Leadership
- Planning and Procedures
- Training, Exercises, and Evaluation
- Activities that Enhance Communications Coordination
- Standards-Based Technology and Infrastructure
- Cybersecurity

2.1 Governance and Leadership

Strong governance and leadership structures are essential to effective decision-making, coordination, and planning for emergency communications. While the existence and development of governance bodies is a significant accomplishment, many of these entities were originally established to address land mobile radio (LMR) interoperability issues. Evolving technology and rising expectations among incident commanders for emergency communications support has driven change in 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 formalizing, expanding, and updating current incident management structures, processes, and investments in governance and leadership.

In FY 2025, grant applicants 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. Formal governance and leadership structures can also facilitate the development of operating procedures and planning mechanisms that establish priorities, objectives, strategies, and tactics during response and recovery operations.[11]

For regional, cross-border initiatives, grant applicants should coordinate projects with national level emergency communications coordination bodies, such as the NCSWIC and the Regional Emergency Communications Coordination Working Groups (RECCWGs). The NCSWIC promotes and coordinates state level activities designed to ensure the highest level of public safety communications access and availability across the nation. RECCWGs are congressionally-mandated planning and coordination bodies located in each FEMA Region and provide a collaborative forum to assess and address the survivability, sustainability, operability, and interoperability of emergency communications systems at all levels of government. Grant-funded investments that are coordinated with these bodies will help ensure that federally-funded emergency communications investments are interoperable and support national policies.

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

[11] See the *National Incident Management System Implementation Objectives* at: fema.gov/emergency-managers/nims.

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

- Develop/sustain the SIGB or SIEC activities and SWIC position or fully-staffed SWIC office
    - In accordance with DHS/FEMA requirements, all states and territories receiving Homeland Security Grant Program funds are required to designate a full-time SWIC with 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
- Formalize and adapt governance structures and processes to address the evolving operating environment to:
    - Include and coordinate with emergency communications leaders (e.g., 911 leaders, IPAWS Program Management Office, FirstNet Authority, RECCWGs, public utilities commissions) and representatives from multiple agencies, jurisdictions, disciplines, levels of government, tribes, rural areas, subject matter experts, and private industry when creating strategic and operational plans and policies, and during training and exercise development and execution
    - Identify and include information management, network infrastructure, and cybersecurity representatives in governance membership or through formalized coordination to undertake technology integration and migration initiatives (e.g., 911, alerts and warnings, broadband, cybersecurity, information management, network infrastructure), as well as identify and address legislative and regulatory issues associated with emerging technology
    - 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
    - Formalize and regularly review cross-jurisdictional, multi-state, or multi-organizational agreements (e.g., memoranda of understanding or agreement [MOU/MOA], automatic and mutual aid agreements) to account for changes to resources, capabilities, and information- or technology-sharing needs
    - Integrate emergency communications governance and leadership into broader statewide planning efforts (e.g., the operationalization, tactical integration, and continued enhancements of public safety broadband capabilities, 911 system technology migration, IT enhancements, commercial broadband, auxiliary communications) 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 that aids in the coordination of messaging within partnering IPAWS Alerting Authorities; improves the common operating picture and achieves greater situational awareness; and increases awareness of existing plans, policies, and procedures

2.2 Planning and Procedures

The public safety community benefits from a comprehensive and inclusive approach to emergency communications planning. The NECP recommends that response agencies seek to improve responders' ability to communicate and share information with others through formal written strategies, plans, and standard operating procedures (SOPs) or guidelines that integrate the capabilities of all users and account for the entire system lifecycle.[12] Through development and updating of their SCIPs, states, tribes, and territories engage multiple jurisdictions, disciplines, and levels of government in planning, incorporating

[12] In addition to SOPs, Standard Operating Guidelines (SOGs) and Field Operations Guides (FOGs) are formal written guidelines or instructions for incident response, including operational and technical components that enable emergency responders to act in a coordinated fashion across disciplines. See CISA's *SAFECOM Writing Guide for SOGs* for more information.

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, including Field Operations Guides, Tactical Interoperable Communications Plans (TICPs), Primary, Alternate, Contingent, and Emergency (PACE) Plans, and FEMA Regional Emergency Communications Plans (RECPs). Field Operations Guides are technical references for emergency communications planning and for technicians responsible for radios that will be used in emergency responses. TICPs are designed to allow urban areas, counties, regions, states/territories, tribes, or federal agencies to document interoperable communications governance structures, technology assets, and usage policies and procedures. PACE Plans delineate the primary, alternate, contingent, and emergency communications networks and resources that will be progressively implemented for continuity or as backup if the day-to-day organic communications capabilities are damaged, destroyed, or otherwise unavailable. RECPs, along with their associated state, territorial, or tribal annexes, serve to identify emergency communications capability shortfalls and potential resource requirements.

Grant applicants are encouraged to leverage these planning resources as a source of input and reference for all emergency communications grant applications and investment justifications. Updating plans and SOPs to address emergency communications gaps, new technologies, and stakeholder needs help 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 broader planning priorities.

In FY 2025, grant applicants should continue to target funding toward planning activities, including updates of local, regional, statewide, tribal, and territory plans, and ensure plans incorporate the capabilities and needs of all emergency communications systems throughout their lifecycles. 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 sustainment, while 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 applicants should target funding toward critical planning activities, including the following:

- Update SCIPs, other strategic and tactical plans, and procedures to:
  - Reflect the NECP strategic goals and objectives into measurable goals, activities, and milestones
  - Incorporate whole community concepts[13]
  - Integrate lifecycle planning to inform agency funding decisions
  - Address capabilities (e.g., voice, video, data), 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
  - Account for NIMS implementation activities including the *NIMS Information and Communications Technology (ICT) Functional Guidance*
  - Identify and address FCC directives affecting current or planned public safety communications systems (e.g., spectrum, licensing, interference)

[13] 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."

  - Incorporate a multifaceted approach to ensure the security, confidentiality, integrity, reliability, and availability of fully interoperable voice and data applications and services
  - Include all components of the emergency communications ecosystem (e.g., 911 systems, auxiliary communications, AWN, broadband networks, LMR, video networks)
- 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 and mitigation
  - Plan and develop shared communication systems and infrastructure projects for improved utilization and integration of available communications assets with partners
  - Develop and perform risk, resiliency, and vulnerability assessments (e.g., cyber, Threat and Hazard Identification and Risk Assessment [THIRA], communications security [COMSEC][14])
  - Incorporate risk management strategies for cybersecurity, continuity, and recovery (e.g., National Risk Index [NRI][15])
  - Integrate emergency communications assets and needs into state-level plans
  - Coordinate with SWIC, broadband coordinator, State Administrative Agency (SAA),[16] and state-level planners (e.g., 911 planners, public utilities commissions) to ensure proposed investments align to statewide plans and comply with identified technical requirements
  - Establish a cybersecurity response plan including continuity of vulnerable communications components and implementing resilient network designs (e.g., segmenting essential functions, strong access controls, multi-factor authentication for staff logins) to limit the impact of cyber incidents
- Identify, review, establish, verify, and improve communications SOPs or guidelines 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, mitigate vulnerabilities, and identify contingencies for the continuity of critical communications

2.3 Training, Exercises, and Evaluation

Results from the SAFECOM Nationwide Survey, AARs, and similar assessments reveal that jurisdictions are better able to respond to emergencies due in part to regular training and exercises. Training, exercises, and evaluations 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 traditional emergency responder disciplines from all levels of government, as well as other entities that share information during emergencies (e.g., public health and medical facilities, utilities, and other critical infrastructure facilities, nongovernmental organizations, private citizens), to practice communications for

[14] COMSEC is a component of security that protects public safety wired and wireless transmissions from unauthorized access. When public safety transmissions include sensitive information related to tactical or investigative law enforcement operations, patient health, or logistics among agencies responding to incidents and disasters, the information may present a vulnerability if not protected. COMSEC provides the necessary structure of protections, ensuring the confidentiality and integrity of critical and sensitive communications.

[15] FEMA developed the NRI as an online tool to help communities analyze risk factors when preparing grant applications. The NRI is available at: fema.gov/flood-maps/products-tools/national-risk-index.

[16] Many designated SAAs administer federal grants, and are responsible for sub-recipient oversight of grant-funded activities.

a whole community response and approach. It also recommends agencies utilize all types of communication technologies and identify gaps and problems with technologies or protocols.

In FY 2025, grant applicants should continue to invest in communications-related training, exercises, and evaluations (in-person and virtual) to address gaps identified in response and recovery operations, which should include thoroughly testing resiliency and continuity of communications. Grant applicants 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 applicants should target funding toward certified training, exercises, and evaluation activities, including:

- Conduct NIMS-compliant training (e.g., training in the Incident Command System [ICS]). Role-specific training for the ICS Communications Unit includes Communications Unit Leader (COML), Communications Technician (COMT), Information Technology Service Unit Leader (ITSL), Radio Operator (RADO), Incident Tactical Dispatcher (INTD), Auxiliary Communications (AUXCOMM), and Incident Communication Center Manager (INCM).[17] Role-specific training for the ICS Information Technology Service Unit includes ITSL and Information Technology Service Specialist (ITSS). Role-specific Cybersecurity Unit training is still under development, but pertinent training is available for this subject matter through the National Cybersecurity Preparedness Consortium[18]
- Improve the ability of states, tribes, and territories to track and share trained Communications and Information Technology (IT) Service Unit personnel during response operations (e.g., include Communications and IT Service Unit training plan within statewide plans such as the SCIP)
- Conduct periodic, recurring training and exercises involving personnel from all levels of government who are assigned to operate communications capabilities, to test communications systems and personnel proficiency (e.g., include emerging technologies and system failure), and utilize third-party evaluators with communications expertise
- Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel, to ensure that responders effectively use and are not overloaded by available information
- Perform exercises that support and demonstrate the adoption, implementation, and use of the NIMS ICT function concepts and principles
- Participate in cross-training and state, regional, or national level exercises to validate plans and procedures to include tribes, nongovernmental organizations, and private sector communications stakeholders
- Provide training and exercises on new and existing systems, equipment, and SOPs or guidelines
- Develop or update training and exercise programs to address new technologies, data interoperability, cybersecurity, encryption, use of dedicated federal, state, local, and national interoperability channels, personally identifiable information, and continuity of communications
- Test communications survivability, resilience, and continuity of communications, to include validation of continuity procedures and operational testing of secondary and backup systems and equipment
- Develop and support instructor cadres to expand training for communications-support personnel
- Assess and update training curriculums and exercise criteria to reflect changes in the operating environment and plain language protocols

[17] 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: fema.gov/emergency-managers/nims/implementation-training.
[18] Web-based training with FEMA cataloged courses may be found at the consortium's website at nationalcpc.org.

- 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 cybersecurity 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 Alerting Authorities incorporating the use of IPAWS

2.4 Activities that Enhance Communications Coordination

There has been significant improvement in capabilities at state, local, tribal, and territorial levels resulting in the ability of jurisdictions to coordinate communications resources and services more effectively during emergency incidents and planned events. This includes the integration of capabilities, resources, and personnel across the whole community. As incidents escalate and evolve, 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 2025, grant applicants are encouraged to update inventories of communications assets and share information within their state, tribe, or territory and region (e.g., neighboring jurisdictions, 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 Communication Assets Survey and Mapping (CASM) Tool—a web-based tool that assists non-federal public safety agencies to collect and visualize data, and assess inter-agency interoperability based on communications assets and interoperability methods.[19] Similarly, to assist in coordinating the use of 700 and 800 megahertz (MHz) public safety frequencies, agencies should use the Computer Assisted Pre-Coordination Resource and Database (CAPRAD) system and work with the FCC 700 and 800 MHz Regional Planning Committees.[20] Grant applicants and recipients should identify gaps in capabilities and target funding toward those gaps.

In addition, CISA recommends that grant recipients implement NIMS ICS principles during all incidents and planned events. In March 2023, FEMA published the *NIMS Information and Communications Technology (ICT) Functional Guidance* to provide instruction on integrating communications, information technology, and cybersecurity functions into the ICS structure while adhering to the concepts and principles of the NIMS doctrine. Grant applicants and recipients are also encouraged to actively engage neighboring jurisdictions—both internal and external to the state, local, 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 applicants should target funding to:

- Promote projects that confirm NIMS implementation, continued use of ICS, incorporation of the *ICT Functional Guidance*, and information sharing:
  - Establish or enhance primary, alternate, contingency, and emergency communications capabilities and share appropriate ICS forms and information illustrating the status of an agency's capabilities

[19] CISA hosts public safety software tools on the SAFECOM website at: cisa.gov/safecom/resources. Tools include the CASM Resource Finder, the electronic National Interoperability Field Operations Guide 2.0 (eNIFOG), and electronic Auxiliary Communications Field Operations Guide (eAUXFOG) mobile applications. Users may request online training from CISA Technical Assistance at: cisa.gov/safecom/ictapscip-resources.

[20] DHS Science and Technology Directorate sponsors the CAPRAD system at: caprad.org.

  - Assess and improve the timeliness of notification, activation, and response of communications systems service providers to support the Incident Commander and Incident Management Team(s) requirements at incidents and planned events
  - Address the evolution and convergence of traditional telephone and radio with IT systems by incorporating the ICT Branch into command and coordination systems and safeguarding incident operations from cybersecurity threats
- Enhance the coordination and effective usage of communications resources
  - Ensure inventories of emergency communications resources are updated and comprehensive, and readily share information about features, functionality, and capabilities of operable and interoperable communication resources with partners
  - Promote assessment of communications assets, asset coordination, and resource sharing
  - Implement or transition existing LMR encryption to the Advanced Encryption Standard (AES) to protect sensitive public safety communications, personally identifiable information, protected health information, and criminal justice information (CJI) and to facilitate secure interoperability
  - Implement projects that promote regional, intra- and inter-state collaboration
  - Support initiatives that engage the whole community, including commercial and non-traditional communications partners (e.g., auxiliary communications, volunteers, utilities)
- Develop or update operational protocols and procedures
  - Develop, integrate, or implement NIMS-aligned SOPs or job aides to facilitate the integration, deployment, and use of communications assets or loaned devices
  - Test communications capabilities and personnel proficiency through training, exercises, and real-world events and address needs identified in statewide plans, AARs, or assessments through comprehensive action plans
  - Review the inclusion and operationalization of NPSBN, also known as FirstNet, and other public safety broadband capabilities to ensure SOPs govern the technologies' use, training, and testing
  - Develop recommended SOPs or guidelines regarding the use of personal communications devices (e.g., bring your own device) for official duties based on applicable laws and regulations
  - Review usage of Priority Telecommunications Services (e.g., Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority), and ensure SOPs govern the programs' use and testing
  - Plan for Alerting Authorities to ensure the highest state of readiness of existing capabilities for resilient and interoperable alerts, warnings, messaging, and notifications using current local, county, state, tribal, territorial, and federal systems, and when applicable, the IPAWS[21]
  - Develop guidelines regarding the use of auxiliary communications devices (e.g., amateur radio, military radio, citizens band radio) for official duties based on applicable laws and regulations[22]
- Strengthen resilience and continuity of communications
  - Inventory and typing of resources and other activities that provide alternate, contingency, and emergency communications solutions (e.g., strategic technology reserve, radio caches, LMR sites on wheels, commercial provider/supplier assets such as cell on wheels [COWs], compact rapid deployables [CRDs])
  - Establish testing and usage observations of personnel proficiency using primary, alternate, contingency, and emergency communications resources

[21] FEMA IPAWS Best Practices, including information on developing an Alert Escalation Process, are available at: fema.gov/sites/default/files/documents/fema_ipaws-best-practices-guide.pdf.

[22] For more information on auxiliary communications guidelines and the SHAred RESources (SHARES) High Frequency Radio program, see: cisa.gov/shared-resources-shares-high-frequency-hf-radio-program.

  - Address system capacity and staffing allocations and availability for continuity of operations planning

2.5 Standards-based Technology and Infrastructure

Public safety agencies continue to maintain and evolve LMR technologies for mission critical voice capabilities, including the pursuit of shared Project 25 (P25) radio systems and infrastructure. With acknowledgment of the need for enhanced data capabilities, many public safety organizations have implemented complementary public safety-focused broadband solutions. In addition, Next Generation 911 (NG911) systems are being deployed and continue to mature. The public safety community continues to develop strategies and technology roadmaps for implementing standards-based, vendor-neutral devices and applications that can sustain service in the demanding public safety operating environment and provide mission critical communications. In addition, public safety agencies must address operability, interoperability, security, and resiliency challenges posed by rapid technology advancements (e.g., 5G, 6G, artificial intelligence [AI], digital identity management, Internet of Things [IoT], geographic information systems) and increased information sharing, ensuring the most critical information gets to the right people at the right time.

In FY 2025, grant applicants should continue to invest in accredited technical standards-based technologies to enable interoperability between agencies and jurisdictions, regardless of provider. Grant applicants should include technical specifications and performance-based requirements in procurement agreements with providers/suppliers and obtain sufficient documentation and testing results to verify that infrastructure, equipment, and software are compliant with applicable standards and that features, functions, and services provide the expected and required interoperability. Grant applicants are strongly encouraged to invest in equipment that will sustain and maintain current capabilities while planning for new technologies and capabilities that may not have fully defined and accredited technical standards. As emergency communications capabilities continue to evolve, applicants should participate in community outreach and planning to ensure new capabilities are interoperable and all user requirements are incorporated.

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

- Sustain and maintain current LMR capabilities based on mission requirements
- Purchase and use P25-compliant LMR equipment (see P25 Compliance Assessment Program [CAP] approved equipment list) for mission critical voice communications[23]
- Support development and deployment of interoperable public safety broadband capabilities by nationwide and regional commercial broadband service providers. Consider using the NPSBN and FirstNet-approved public safety broadband capabilities, devices, and applications dedicated for public safety using multi-layered, proven cybersecurity and network security solutions[24]
- Transition towards NG911 capabilities in compliance with NG911 standards[25]
- Transition LMR encryption capabilities to full P25 AES 256-bit for all LMR systems establishing encrypted interoperability where applicable
- Support technical standards that allow for interoperability of alerts, warnings, and notifications across different systems

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

[24] Applicants interested in using FirstNet for broadband investments should consult with the FirstNet Authority to ensure investments meet all technical requirements to operate and interoperate on the NPSBN. Refer to the Authority’s contact information at: firstnet.gov.

[25] For more information, see the *NG911 Standards Identification and Review*: 911.gov/issues/ng911/standards-for-enhanced-and-next-generation-911/.

- Secure and protect equipment, information, and capabilities from physical and cyber threats
- Acquire, sustain, and maintain Common Alerting Protocol-compliant software that meets IPAWS requirements
- Employ standards-based information exchange models and data sharing solutions
- Secure standards-based interconnectivity gateway subsystems
- Sustain and ensure critical communication systems connectivity and resiliency, including backup solutions, among key government leadership, internal elements, other supporting organizations, and the public
- Support standards and practices that enhance survivability and resilience to electromagnetic effects
- 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 communications capabilities (e.g., auxiliary communications gateway equipment, backup power, High Frequency [HF] radios, repeaters, satellite devices)
  - 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

2.6 Cybersecurity

As cyber threats and vulnerabilities grow in complexity and sophistication, incidents become more numerous and severe against emergency communications systems. Therefore, it is critical that public safety organizations take proactive measures to carefully manage their cybersecurity risks. To prepare for cyber incidents, the public safety community must continually identify risks and evolve security requirements in coordination with partners. Cybersecurity is a shared mission across all levels of government, the private sector, nongovernmental organizations, public safety communications end-users, and the public.

In FY 2025, grant applicants should invest in solutions that enhance their cybersecurity posture. Cybersecurity must be addressed through planning, governance, training and exercise, and technology solutions that secure networks. Applicants should ensure cybersecurity planning is comprehensive and maintained throughout the lifecycle of all network components. Cybersecurity risk management should also include updates to non-technology support activities, such as mutual aid agreements, SOPs, policy development, and training and education. Personnel should be trained on the latest security, resiliency, continuity and operational practices and maintain in-service training as new technology and methods are made available. Personnel should also be educated in cyber hygiene and best practices to prevent, detect, and deter cybersecurity risks whether they are natural or technological in nature, accidental or intentional.

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

- Develop and maintain cybersecurity risk management
- Implement the CISA *Cyber Essentials Toolkits*[26]
- Implement the NIST Cybersecurity *Framework*[27] to complement an existing risk management process or to develop a credible program if one does not exist. The framework establishes six functions to integrate cybersecurity into mission functions and operations, including:
  1) **Govern**: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored;

[26] CISA *Cyber Essential Toolkits* are available at: cisa.gov/resources-tools/resources/cyber-essentials-toolkits.

[27] NIST released the *Cybersecurity Framework* 2.0, 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 and reference tools, see: nist.gov/cyberframework.

2) **Identify**: The organization's current cybersecurity risks are understood;
3) **Protect**: Safeguards to manage the organization's cybersecurity risks are used;
4) **Detect**: Possible cybersecurity attacks and compromises are found and analyzed;
5) **Respond**: Actions regarding a detected cybersecurity incident are taken; and
6) **Recover**: Assets and operations affected by a cybersecurity incident are restored

- Employ the *Cyber Resiliency Resources* available for public safety[28]
- Reference CISA's cybersecurity resources for 911 projects[29]
- Identify and implement standards for cybersecurity that fit system and mission needs while maintaining operability and interoperability
- Develop incident response plans, recovery plans, resiliency plans, and continuity of operations plans in anticipation of physical or cybersecurity incidents[30]
- Mitigate cybersecurity vulnerabilities with consideration of the potential impacts of cybersecurity risk management on interoperability with the broader community
- Identify and mitigate equipment and protocol vulnerabilities
- Plan and deploy AES 256-bit encryption capabilities for all LMR systems including link layer authentication and link layer encryption (when available)
- Implement the Communications Security Reliability and Interoperability Council (CSRIC) cybersecurity best practices for public safety entities[31]
- Implement Phishing Resistant Multi-Factor Authentication (MFA)[32]

[28] CISA *Cyber Resiliency Resources* are available at: cisa.gov/resources-tools/resources/communications-and-cyber-resiliency-toolkit.

[29] CISA cybersecurity resources for NG911 projects are available at: cisa.gov/911-cybersecurity-resource-hub.

[30] CISA *Cyber Incident and Cyber Vulnerability Playbooks* are available at: cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

[31] CSRIC is an advisory committee of the FCC that provides recommendations to ensure the security, reliability, and interoperability of communications systems. The CSRIC cybersecurity best practices for public safety entities are available using the search tool opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data after selecting 'Public Safety' in Industry Role(s) filter and 'Cyber Security' in Keywords filter.

[32] Phishing resistant MFA requirements are available within NIST 800-63-4. For general MFA information, see CISA resources at: cisa.gov/resources-tools/resources/multi-factor-authentication-mfa.

3. Before Applying

SAFECOM encourages potential emergency communications grant applicants to:

- Review the NECP and SCIP
- Coordinate with statewide emergency communications leaders
- Recognize changes in the emergency communications ecosystem
- Understand applicable 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 ensure proposed projects support national goals and objectives. Similarly, grant applicants should review their state or territory's SCIP (and other applicable plans) to ensure proposals support statewide plans to improve communications across all emergency communications systems and capabilities. Some DHS grants (e.g., Homeland Security Grant Program) require applicants to align project activities to their SCIP, so it is a best practice for all applicants to describe how proposed projects align with the needs identified in their strategic plans and performance measures.

3.2 Coordinate with Statewide Emergency Communications Leaders

To ensure projects are compatible, interoperable, and support statewide plans and strategies, grant applicants 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., Emergency Management Agency Director, 911 Administrator, Homeland Security Director, Statewide/Regional Communications System Owners/Operators, SAAs), as well as require applicants to attach a letter of project support from these leaders. Grant applicants should also consult the SIGB or SIEC, as they serve as the primary steering group for the statewide voice and data interoperability strategy. Additionally, grant applicants 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

Grant applicants 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 technologies, national policies and laws, spectrum issues, and the reduction and streamlining of grant programs.

Developments in Technologies

Traditionally, LMR systems are the primary capabilities the public safety community uses to achieve mission critical voice communications in the field. To augment their LMR capabilities, emergency response agencies are increasingly using Broadband Push-To-Talk (PTT) voice services and high-speed data services available from the FirstNet and other commercial broadband service providers. Internet Protocol (IP)-enabled networks have transformed how public officials 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 enables increased resilience and redundancy in call routing and information sharing. Also, the deployment of a nationwide emergency alerting system is using both traditional media, such as broadcast and cable, as well as IP-based technologies to transmit alerts to mobile telephones and other devices.

Public safety IT systems include sensitive data, such as law enforcement CJI and electronic healthcare records, which require robust security considerations including end-to-end encryption, storage, access, and authentication. While electronic access to this data enables more effective response operations, it also exposes risks including system failures, lack of user or server connections, ineffective or lack of cyber protections, and vulnerability to attacks by malicious hackers. As the community adopts new technologies and applications, it too must increase understanding and planning for the security risks associated with the increasingly interconnected architecture and vast complexity of IP-based technologies and services.

To protect against phishing, malware, and other potential threats, a multifaceted cybersecurity risk management approach is needed to ensure the confidentiality, integrity, and availability of communications system and sensitive data. For example, comprehensive cybersecurity training and education on the proper use and security of devices, services, and applications will be required. In addition, planning must match user needs against bandwidth requirements and the options for network resiliency. Critical cybersecurity controls such as phishing resistant MFA should also be implemented.

The convergence of technologies and risks in this evolving ecosystem shows the importance of ongoing planning for emergency communications. Grant applicants and their respective governance and leadership should 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, grant applicants should prioritize maintaining LMR systems and other emergency communications capabilities gained in recent years as they adopt, deploy, and integrate IP-based technologies and services.

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. A non-exhaustive list of applicable laws include the Infrastructure Investment and Jobs Act and the American Rescue Plan Act.

- ***Infrastructure Investment and Jobs Act.*** Signed into law on November 15, 2021, the Infrastructure Investment and Jobs Act provided over $1.2 trillion in broadband, public works, and transportation infrastructure funding. Specifically, the Act authorized several new grant programs and policies that may be relevant to the public safety community. Grant applicants are encouraged to review these federal financial assistance opportunities for applicability to emergency communications projects, as they become available.

- ***American Rescue Plan Act.*** Signed into law on March 11, 2021, the American Rescue Plan Act provided funding for state, local, tribal, and territorial governments to mitigate the effects of the COVID-19 pandemic. Additional appropriations included supplemental funding for existing federal emergency management grant programs. Grant applicants are encouraged to review funding opportunities for emergency communications projects, as authorized through this Act.

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, the FirstNet Authority holds the FCC license for the 700 MHz public safety broadband spectrum to deploy the NPSBN. Grant applicants seeking federal funds for emergency communications projects should be aware of initiatives and actions affecting spectrum use for public safety entities. Applicants 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,[33] SWIC), the FCC, and/or the FirstNet Authority early in the project development process to determine whether the grant applicant will have authority to operate in the desired spectrum, once complete. Key spectrum-related issues are described below:

- **Very High Frequency (VHF)/Ultra-High Frequency (UHF) Narrowbanding.**[34] The FCC mandated all non-federal LMR licensees operating between 150 and 512 MHz and using 25 kilohertz (kHz) bandwidth voice channels to migrate to 12.5 kHz bandwidth or equivalent efficiency by January 1, 2013. Grant applicants should confirm 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. Grant applicants that have not complied with the FCC narrowband mandate may face limitations on their eligibility for federal funding.[35] Grant applicants that are operating on 25 kHz bandwidth voice channels pursuant to a waiver should provide a copy of the waiver as well as a description of how the applicant intends to come into compliance upon the expiration of the waiver.

- **4.9 gigahertz (GHz)**. The FCC mandated that all incumbent licensees operating in the 4.9 GHz band as of January 18, 2023, submit granular technical data on their existing operations into the FCC's Universal Licensing System (ULS). On December 9, 2024, two FCC Bureaus released a Public Notice instructing incumbent licensees how to submit such data.[36] The Bureaus gave incumbents six months to complete the data submission.[37]

- **5.9 GHz.** In 2020, the FCC repurposed the 5.9 GHz band by designating the lower 45 MHz of the band (5.850–5.895 GHz) for unlicensed operations while continuing to dedicate the upper 30 MHz for Intelligent Transportation Service (ITS) operations. In the process, the FCC modified existing ITS licenses to permit operation only in the upper 30 MHz portion of the band. The FCC also required that all ITS licensees cease operations in the lower 45 MHz of the band by July 5, 2022, and file a notification confirming their timely exit by July 20, 2022. Where licensees failed to timely transition out of the lower 45 MHz as evidenced by their failure to notify the FCC, those licenses terminated automatically. Additionally, the FCC required ITS operations in the upper 30 MHz to transition from dedicated short-range communications-based technology to cellular vehicle to everything-based technology as the connected mobility platform for implementing the future of ITS communications in the United States.

In general, grant applicants 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

[33] For more information on frequency coordinators, see: fcc.gov/general/public-safety-frequency-coordinators.
[34] For more information on narrowbanding, see: fcc.gov/narrowbanding-overview.
[35] See "Guidance for licensees for FCC's narrowband operation requirement" at: fcc.gov/document/guidance-licensees-fccs-narrowband-operation-requirement. Grant applicants with questions on narrowbanding may contact the FCC at ULS support: 1-877-480-3201.
[36] The FCC Public Safety and Homeland Security Bureau and Wireless Telecommunications Bureau Establish Deadline for 4.9 GHz Public Safety Licensees to Provide Granular Licensing Data, Public Notice, DA 24-1137 (December 9, 2024).
[37] The six-month time period for submission of granular data expires on June 9, 2025.
[38] Contact the FCC's Public Safety Homeland Security Bureau at pshsbinfo@fcc.gov.
[39] While federal licensing fees are generally *not* allowable under most federal grants, public safety entities are often exempt from FCC filing fees. For more information, see: fcc.gov/licensing-databases/fees.

- 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

Over the past decade, the fluctuation of grants funding emergency communications (e.g., elimination of dedicated funding streams in favor of consolidated programs, required spending on federal priorities) has increased competition for funding. Understanding that grants are in high demand, emergency communications leaders and agencies are strongly encouraged to work with other jurisdictions and disciplines to coordinate resources and projects, facilitate asset-sharing, and avoid duplication of activities. Additionally, when developing funding proposals, grant applicants 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. 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 Applicable Federal Grant Requirements and Restrictions

Federal Grant Requirements

Emergency communications grants are administered by numerous federal agencies in accordance with various statutory, regulatory, 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
- Accredited technical standards preferred, required, or allowed under each program, if applicable

[40] Consult the grant officer as some federal grants do not allow construction or ground-disturbing activities.

[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: fcc.gov/general/800-mhz-spectrum. 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 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* or the *Funding Mechanisms Guide for Public Safety Communications*, posted to the SAFECOM website at: cisa.gov/safecom/funding.

- 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 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 that they meet, or are working to meet, the most recent NIMS implementation and reporting requirements as described in the applicable Notice of Funding Opportunity and NIMS Implementation Objectives published by FEMA.[45]

- **Stakeholder Preparedness Review (SPR) Submittal.** The Stakeholder Preparedness Review replaces the State Preparedness Report. Section 652(c) of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109-295), 6 U.S.C. §752(c), and requires any state, territory, urban area, or tribe that receives federal preparedness assistance administered by DHS to submit an annual SPR to FEMA. The SPR is a self-assessment of a jurisdiction's current capability levels against the targets identified in the THIRA. Jurisdictions use the SPR to estimate their current preparedness capabilities and compare those to their THIRA results to identify gaps. They also use the SPR to identify potential approaches for addressing those capability gaps.

- **Threat and Hazard Identification and Risk Assessment.** Since 2019, DHS/FEMA has required Homeland Security Grant Program (State Homeland Security Program and Urban Area Security Initiative), Tribal Homeland Security Grant Program, and Emergency Management Performance Grant Program recipients to complete a THIRA report every three years (previously, a THIRA was required annually). Grant recipients are also required to submit an SPR annually. Communities use the THIRA process to better understand their risks and determine the level of capabilities needed to address those risks. Through the THIRA process, communities set goals for building and sustaining their capabilities. It results in whole community-informed capability targets and resource requirements necessary to address anticipated and unanticipated risks.[46]

  Developing and updating an effective THIRA/SPR requires active involvement from the whole community. This can result in more complete, accurate, and actionable assessments and planning efforts. Therefore, recipients should actively engage a wide variety of stakeholders in the THIRA/SPR process. Emergency communications subject matter experts should be involved in the THIRA/SPR process and provide input as appropriate, including but not exclusive to the potential impacts of threats and hazards on emergency communications. For additional information, refer to each grant program's Notice of Funding Opportunity or the *Preparedness*

[44] While these are common requirements that affect many emergency communications grants, they may not apply to all grants; applicants should consult their grant guidance and grant officer for specific questions on grant requirements.
[45] The NIMS Implementation Objectives reflect the concepts and principles contained in NIMS and clarify the NIMS implementation requirements in FEMA preparedness grant Notices of Funding Opportunity. As recipients and sub-recipients of federal preparedness (non-disaster) grant awards, jurisdictions and organizations must achieve, or be actively working to achieve, all of the NIMS Implementation Objectives. Additional NIMS implementation guidance can be found at: fema.gov/emergency-managers/nims/implementation-training.
[46] For additional information on the THIRA process, see: fema.gov/emergency-managers/national-preparedness/goal/risk-capability-assessment.

Grants Manual[47] for reporting requirements, including the THIRA/SPR. Grant recipients participating in risk assessments are strongly encouraged to:

  - Analyze communications gaps, excesses, and deficiencies within the state regularly
  - Utilize THIRA to identify communications-specific threats and hazards and set core capability targets identified in the *National Preparedness Goal*
  - Ensure THIRA updates include outcomes as stated in program guidance
  - Assist with the development of the SPR

- **Nationwide Cybersecurity Review.** Recipients and sub-recipients of State Homeland Security Program and Urban Area Security Initiative awards are required to complete the Nationwide Cybersecurity Review, enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The CIO, CISO, or equivalent of each recipient and sub-recipient should complete the Nationwide Cybersecurity Review. If there is no CIO, CISO, or equivalent, the most senior cybersecurity professional should complete the assessment.[48]

- **National Defense Authorization Act of 2019 Compliance.** Recipients must comply with the requirement prohibiting the procurement, or extending or renewing a contract to procure or obtain "any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system," on or after August 13, 2019, unless an exception applies or a waiver is granted.

- **Reporting.** Federal agencies are improving how they demonstrate the impact and effectiveness of federal grant programs. 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 applicable 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 some common restrictions on federal grant funding and should consult the grant officer with any questions, particularly as requirements vary by program. This list is for awareness purposes only and is not meant to be an exhaustive list of restrictions.

- **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. In addition, federal funds cannot purchase or pay for the same cost or activity already paid for from another source of funding (e.g., insurance claim). This is

[47] DHS/FEMA developed a *Preparedness Grants Manual* to guide grant applicants and recipients on how to manage their grants and other resources, available at: fema.gov/grants/preparedness/manual.

[48] The Nationwide Cybersecurity Review is completed on the Multi-State Information Sharing and Analysis Center. For more information, visit cisecurity.org/ms-isac/services/ncsr or email ncsr@cissecurity.org.

referred to as a prohibition on the duplication of benefits or "double-dipping." The accounting systems of all recipients and sub-recipients must ensure federal funds are not commingled with funds from other awards or federal agencies, nor duplicate benefits.

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

- **Funding and Sustaining Personnel.** In general, the use of federal grant funding to pay for staff regular time is considered personnel and may be allowable. Recipients are encouraged to refer to the applicable grant program guidance and develop a plan to sustain critical communications positions in the event federal funds are not available to support the position in future years.

- **Supplanting.** Most grant funds cannot supplant (or replace) funds previously allocated 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. Review applicable grant program guidance for specific rules on supplanting.

4. Eligible Activities

The following section details potentially 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 each individual program for more information on 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 program's 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 technologists)

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

[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.

  - 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 who will:
  - Assess immediate needs and future requirements
  - Plan and conduct in-person or virtual exercises in accordance with NIMS and the Homeland Security Exercise and Evaluation Program (HSEEP)
  - Implement NECP goals, objectives, and success indicators
  - 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. Recipients should ensure funding for critical communications positions is sustained after the grant period of performance has ended and core capabilities are maintained.

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 applicants are strongly encouraged to assess needs before planning projects, and to carefully plan projects before purchasing equipment. It is important to review the eligible costs for emergency communications related grants to determine if the below are eligible planning costs.

Potential 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
  - TICPs, FEMA RECPs, or other tactical or regional communications plans
  - Disaster emergency communications plans
  - Communications system lifecycle planning, including migration planning and use of the *Emergency Communications System Lifecycle Planning Guide*[51]
  - Plans for broadband integration with broader communications capabilities
  - Planning projects to share communications and infrastructure resources with partners
  - 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, PACE Plans)
  - Planning for training and exercises
  - Identifying physical and cyber security measures for communications networks and systems

[51] For guidance on emergency communications system lifecycle planning, see: cisa.gov/safecom/funding.

- Planning activities for the transition of 911 to NG911 (e.g., *NG911 Self-Assessment Tool*[52])
- Planning for transitions to P25 AES 256-bit encryption and comprehensive encryption key management capabilities for LMR systems, including implementation of link layer authentication and link layer encryption (when available)
- Planning for cross jurisdictional alerting
- Plans for issuing alerts, warnings, and notifications (e.g., Wireless Emergency Alerts)

- **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 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.[53] Coordination and planning benefit from including a variety of traditional and non-traditional entities supporting public safety, such as tribes, healthcare and public health facilities, alerting authorities, nongovernmental organizations, public works, utilities, forestry services, military, private sector, and the American Red Cross. Including these under-represented organizations or sectors will assist with the development of strategic, operational, and contingency plans. 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 communications interoperability governing bodies.** Strong governance structures and leadership are essential to effective decision-making, coordination, planning, and managing of emergency communications initiatives. Grant 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 MOUs and MOAs 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 governance programs and other decision-making offices, bodies, and individuals that oversee new technology deployments in states, territories, localities, and tribes

[52] SAFECOM/NCSWIC developed a dynamic *NG911 Self-Assessment Tool* for use by state, regional, and local emergency communications centers (ECCs)/public safety answering points (PSAPs) personnel. For more information or to download this tool, see: 911.gov/projects/ng911-self-assessment-tool.

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

- **Development of emergency communications assessments and inventories.** Grant recipients are encouraged to allocate grant funding to planning activities, such as assessments of:
    - Technology capabilities, infrastructure, and equipment (e.g., updating the CASM Tool, creating LMR, LTE, and 5G fleet maps, *NG911 Self-Assessment Tool*)
    - SOPs, coordination of interoperability channels, and regional response plans
    - Training and exercises
    - Spectrum regulatory compliance assessments and system coverage analysis
    - Cost maintenance modeling for equipment and usage
    - Implementation and maintenance of identity, credential, and access management (ICAM) capabilities, including phishing resistant MFA solutions

- **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-state 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 disaster or emergency scenarios
    - Field Operations Guides and templates for Field Operations Guides

- **Planning activities for emerging technologies.** Grant funds may be used to plan for the operationalization of NPSBN/FirstNet, other public safety broadband capabilities, and advanced technologies (e.g., 5G, 6G, AI, NG911, IoT/sensors, wireless mesh, LoRaWAN, WiFi 6/6E), including new devices, applications, services, and infrastructure. Activities may include:
    - Defining users' immediate technology needs and future requirements
    - Updating SCIPs to incorporate high-level goals and initiatives
    - Continued collection of technology usage data, use cases, and needs analyses
    - Developing agreed-upon standards for the use of common applications to promote enhanced level of situational awareness
    - Preliminary planning for implementation, operations, policy, acquisition, and tactical integration of technologies
    - Conducting assessments of cyber risks and strategies to mitigate vulnerabilities
    - Implementing identity management solutions to address growing data management, interoperability, and cybersecurity challenges, with consideration for federated solutions, such as the *Trustmark Framework*[54]
    - Collecting and reporting granular 4.9 GHz technical and licensing data per the FCC's rules
    - Enhancing LMR encryption interoperability and capabilities through comprehensive transition to P25 AES-256 encryption with effective shared encryption key management capabilities across all levels of government
    - Testing and evaluation of technologies for operability, interoperability, security, and resilience in advance of deployment

[54] For more information on identity, credential, and access management and the *Trustmark Framework*, see: cisa.gov/safecom/icam.

- **Use of priority communications service programs.** Grant funds may be used to assist priority service planning and engineering, and to facilitate participation in federal priority service programs,[55] including:
  - Government Emergency Telecommunications Service (GETS)
  - Wireless Priority Service (WPS)
  - Telecommunications Service Priority (TSP)

- **Use of alerts, warnings, and notifications.** Grant funds may be used to acquire mass notification alert systems that include IPAWS[56]:
  - Emergency Alert System (EAS)
  - Wireless Emergency Alerts (WEA)
  - Non-Weather Emergency Messages via National Weather Service All Hazards Weather Radio
  - Internet-based services
  - Unique and local alerting systems

  In addition to distributing AWNs through EAS, WEA, and Weather Radio, IPAWS supports Internet-based products and services that redistribute alerts via the IPAWS All Hazards Information Feed. Examples include digital signage, wireless device applications, desktop alerting, assistive devices, and siren systems.

Additional Requirements and Recommendations for Planning Activities

Additional activities in support of federal planning initiatives include updating and submitting a SPR, THIRA, and SCIP, as well as demonstrating NIMS implementation.[57]

4.3 Training

Potential Training Costs

When allowable under the grant award, 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 SCIPs. Recipients should continue to train and improve personnel efficiency on LMR systems as it is necessary to ensure public safety officials can achieve mission critical voice communications. As public safety agencies integrate other communications technologies into operations, the need for training becomes even more critical to ensure response personnel are maximizing all capabilities. Training projects should be consistent with the NECP priorities and address gaps identified through SCIPs, TICPs, PACE Plans, AARs, and other assessments. Training reinforces SOPs and proper equipment use and proficiency by personnel. Grant recipients are strongly encouraged to include training in projects that involve new SOPs or equipment purchases.

- **Development, delivery, attendance, and evaluation of training.**[58] Grant funds may be used to plan, attend, and conduct communications-specific training workshops or meetings to include

[55] For more information on priority services, see: cisa.gov/resources-tools/programs/priority-telecommunications-services.

[56] For more information on IPAWS, see: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system.

[57] For more information on the *Preparedness Grants Manual*, see: fema.gov/grants/preparedness/manual.

[58] DHS training catalogs are available at: dhs.gov/training-technical-assistance. CISA Service Catalog is available at: cisa.gov/resources-tools/services. The federal-sponsored and state-sponsored course catalogs can be found at: firstrespondertraining.gov/frts/.

costs related to planning, meeting space, and other logistics costs, facilitation, travel, and training development. Communications-specific training should focus on the following:

  - Use of SOPs and other established operational protocols (e.g., common language)
  - NIMS/ICS training
  - Any ICS Communications Unit/Information Technology Service Unit position-specific training (e.g., COML, COMT, ITSL, ITSS, RADO, INTD, AUXCOMM, INCM)
  - Information for elected officials and decision-makers to understand public safety communications and requirements
  - 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 or updates of CASM Tool
  - Integration of technologies into public safety operations
  - Cybersecurity and physical security education

- **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, name badges, materials)
  - Software programs and applications to enable remote learning

Additional Requirements and Recommendations for Training Activities

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

- **NIMS Implementation.**[59] 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/Information Technology Service Unit Leader and other ICS Communications Unit/Information Technology Service Unit Training.** CISA, in partnership with FEMA's National Integration Center, the DHS Science and Technology Directorate, and practitioners from across the country, developed performance and training standards for the All-Hazards COML/ITSL and formulated a curriculum and comprehensive All-Hazards COML/ITSL Course. Recipients should target grant funding toward this training to improve on-site communications during emergencies, as well as satisfy NIMS training requirements.

- **Recommended 911 Minimum Training for Telecommunicators.** The National 911 Program facilitated a project to establish universally accepted minimum training guidelines to be used for aspiring and current 911 telecommunicators, and to provide the foundation for ongoing professional development. The *Recommended Minimum Training Guidelines* identify the minimum topics to be included in any telecommunicator training program.

- **Training offered through the National Cybersecurity Preparedness Consortium (NCPC).** The consortium consists of five partner universities whose mission is to provide research-based, cybersecurity-related training, exercises, and technical assistance to local jurisdictions, counties,

[59] 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: fema.gov/emergency-managers/nims.

states, and the private sector.[60] The NCPC offers both online and instructor-led training that provides successful students with certificates recognized by FEMA.

- **Online Cybersecurity Training.** CISA Learning offers no cost online cybersecurity training on topic such as cloud security, ethical hacking and surveillance, risk management, malware analysis, and more. CISA Learning is available for federal, state, local, tribal, and territorial government agencies, U.S. military personnel and veterans, and the public.

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, fire services, law enforcement, public safety telecommunicators, interoperability coordinators, key information technology and cybersecurity personnel, healthcare and public health officials, public works, 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.

Recommended 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[61]

- **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.[62]

[60] For more information about the NCPC, its partners, and offerings, visit nationalcpc.org.

[61] The FirstNet Authority developed the Broadband Exercise Inject Catalog, providing realistic, consistent, and accurate exercise questions and injects to promote integrating wireless broadband capabilities into public safety training opportunities. The catalog is compatible with HSEEP Master Scenario Events List templates, easily searchable, and can be used for both discussion-based and operations-based exercises. Email the FirstNet Authority at FirstNetExercises@firstnet.gov to receive the latest version of the Broadband Exercise Inject Catalog.

[62] HSEEP resources are available at: fema.gov/emergency-managers/national-preparedness/exercises/hseep.

- **Implementation of 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 for state, local, tribal, and territorial recipients. DHS/FEMA recipients should review NIMS implementation criteria and ensure all federally funded training and exercise activities align with NIMS standards.

- **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. Grant recipients are strongly encouraged to invest in accredited technical standards-based equipment that supports statewide plans for improving emergency communications and interoperability among systems.

Examples of Potentially Allowable Equipment Expenses

- **Design, construction,[63] implementation, enhancement, replacement, maintenance, and disposition of emergency communications systems and equipment, including:**
  - System engineering requirements
  - As-is and proposed enterprise architectures
  - Interoperability feature, function, and capability verification and validation testing plans
  - System lifecycle plans
  - Migration/transition to approved, open architecture, accredited standards-based technologies (e.g., P25 AES encryption)
  - Integration of existing capabilities and advanced technologies (e.g., 5G, 6G, AI, NG911, IoT/sensors, wireless mesh, LoRaWAN, WiFi 6/6E)
  - Integration of cybersecurity tools and services (e.g., cyber appliance insertion, firewalls, hardware and software implementation, malware protection, security information and event management, taps and probes, two-factor authentication, web application firewalls)
  - Analysis and monitoring of cybersecurity and physical security risks
  - 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 wireless and satellite user fees when used for backup communications

- **Use of narrowband equipment.** The FCC mandated all non-federal LMR licensees operating between 150 and 174 MHz, 421–470 MHz, and using 25 kHz bandwidth voice channels to migrate to 12.5 kHz bandwidth or equivalent efficiency by January 1, 2013 (except where narrowband waivers have been permitted). Grant recipients operating wideband pursuant to a waiver should prepare existing systems for eventual compliance upon the expiration of the waiver by prioritizing 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

[63] 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.

- **Site upgrades for emergency communications systems.**
    - Installing or expanding battery backup, generators, solar panels, fuel systems, and grounding systems
    - Evaluating existing shelter space for new communications equipment
    - Conducting tower loading analysis to determine feasibility of supporting new antennas and equipment, as well as tower hardening or replacement to withstand harsh environmental conditions
    - 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., alarm systems, biometrics, fences, keyless entry systems, lighting, monitoring, protective measures, shelter access hardening, smart cards, surveillance cameras)
    - Evaluating and upgrading Public Safety Answering Points, Emergency Communications Centers, and other 911 infrastructure sites to determine requirements and deploy NG911 hardware and software upgrades

- **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, wireless, or cable at communications sites and existing public safety facilities)
    - Analyzing existing IP backbone to determine gaps in supporting high bandwidth public safety communications systems access, connectivity, and applications
    - Planning and modeling network capacity to ensure backhaul links and aggregation points are appropriately provisioned
    - Upgrading existing backbone to support advanced Quality of Service capabilities
    - Installing fiber optic connections and microwave connectivity to support enhanced communications, networking capabilities, and redundancy requirements
    - Ensuring robust cybersecurity protocols and physical security protections are in place
    - Assessing and documenting usage of wireless communications capabilities including:
        - Mobile/wireless data systems facilitated through government-owned or commercial broadband services
        - Applications
        - Devices or platforms supported
        - Speed/capacity/coverage
        - Accessible data
        - Redundancy and resiliency of systems or services
        - Cost of services and systems
        - Existing gaps in capabilities, connectivity, coverage, or application support
        - Standards-based mission critical solutions, including voice, video, and data

- **Purchase of:**
    - Standards-based interoperable communications equipment listed on the Authorized Equipment List (AEL)[64]
    - P25 standards-compliant radio equipment listed on the P25 CAP Approved (Grant-Eligible) Equipment List[65]

[64] For a list of equipment typically allowed by DHS/FEMA grants, see: fema.gov/grants/tools/authorized-equipment-list. The AEL consists of 21 equipment categories further divided into sub-categories and individual items.

[65] For a list of P25 compliant radio equipment, see: dhs.gov/science-and-technology/approved-grant-eligible-equipment.

- Broadband user equipment on the NIST List of Certified Devices[66]
- Broadband applications, services, and equipment that meet appropriate protocols and standards for access to, use of, or compatibility with the NPSBN/FirstNet[67]
- Broadband data and voice cache communications capabilities (e.g., in-vehicle routers, multi-access edge computing, private 5G, Wi-Fi hotspots, and other devices) that augment network access and enable operations in areas where network coverage is challenging or there is an increased need for access and throughput
- 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)
- Software that is IPAWS-compliant to issue alerts, warnings, and notifications to the public
- Physical security equipment (e.g., biometric accesses control systems, door locks)
- Cybersecurity equipment (e.g., cyber appliances, taps and probes, phishing resistant hardware authenticators)
- Auxiliary communications equipment (e.g., amateur radios, HF, satellite devices, SHARES gateways) and operations support (e.g., unmanned aircraft systems [UAS])

Additional Requirements and Recommendations for Equipment Purchases

Some equipment purchases made with federal funds might incur additional requirements. These requirements potentially include:

- **Assignment of full-time Statewide Interoperability Coordinator.** DHS/FEMA requires all states and territories that use 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 CISA 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 accredited 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.[68] Other federal grants require recipients to explain how their procurements will comply with applicable technical standards or provide compelling reasons for using non-standards-based solutions. Recipients should document all purchases and evidence of compliance with standards-based requirements and verify compliance and interoperability through comprehensive testing.

[66] For a list of NIST certified devices, see: nist.gov/ctl/pscr/process-document-nist-list-certified-devices.

[67] For a full list of broadband applications, services, and equipment that meet appropriate protocols and standards for access to, use of, or compatibility with the NPSBN/FirstNet, go to FirstNet.com or contact the FirstNet Authority at info@firstnet.gov.

[68] 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 are met. DHS/FEMA grant recipients must adhere to compliance requirements specified in *SAFECOM Guidance* Appendix D.

- **Compliance with FCC Requirements.** Applicants 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. Contact the FCC at PSHSBinfo@fcc.gov.

- **Compliance with federal EHP laws and policies.** CISA recommends that grant recipients ensure federally-funded projects comply with relevant EHP laws. Construction and installation of communications towers and other ground-disturbing activities frequently require 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.[69]

- **Adoption of new technologies.** Recipients are encouraged to migrate to approved, open architecture, accredited standards-based systems and to integrate existing and other advanced technologies, applications, and software to expand communications capabilities among emergency response providers.

- **Sustainment of current LMR capabilities.** Grant recipients are strongly encouraged to sustain current LMR capabilities for mission critical voice capabilities so that systems continue to deliver highly available and reliable communications.

- **Compliance with covered telecommunications restrictions.** Grant recipients should be aware of restrictions on the procurement and use of certain covered telecommunications equipment because of the John S. McCain National Defense Authorization Act of 2019 and subsequent legislation. In compliance with the Act, federal grant funds obligated by executive agencies may not be used to procure, obtain, extend, renew, or enter into a contract with certain covered telecommunications providers. The FCC maintains the list of communications equipment and service providers deemed threats to U.S. national security at fcc.gov/supplychain/coveredlist.

- **Compliance with prohibitions on covered unmanned aircraft systems from foreign entities.** Recipients must comply with the American Security Drone Act of 2023, enacted as part of the National Defense Authorization Act of 2024, prohibiting the use of federal funds to procure or operate covered UAS from covered foreign entities. The Federal Acquisition Security Council maintains the list of covered foreign entities on SAM.gov.[70]

- **Promotion of regional capabilities.** Grant recipients should coordinate and collaborate with agencies from neighboring municipalities, counties, intra-state regions, contiguous states, and interstate regions to facilitate regional operable and interoperable solutions, including shared infrastructure solutions.

- **Development of communications system lifecycle plans.** Emergency response agencies must upgrade and maintain communications systems to ensure effective operation. Some programs require recipients to submit system lifecycle plans for equipment purchased with federal grant

[69] 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: energy.gov/nepa/downloads/40-cfr-1500-1508-ceq-regulations-implementing-procedural-provisions-nepa-ceq-1978.

[70] UAS resources include *Cybersecurity Guidance Chinese-Manufactured UAS*, *Department of Defense Blue UAS Policy and Cleared List*, *Public Safety Uncrewed Aircraft System Resource Guide*, and *Responding to Drone Calls: Guidance for Emergency Communications Centers*.

funds. As a result, recipients should develop a system lifecycle plan for any communications system.

- **Understanding of cost share.** Federal grants often require recipients to provide a percentage of the total costs allocated to equipment. Federal funds under many programs 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. Grant recipients should refer to the applicable grant guidance and consult the awarding agency with any questions regarding cost share requirements.

5. Emergency Communications Systems and Capabilities

Emergency communications are accomplished through many technologies, each with varying capabilities, standards, and features. When procuring equipment, software, and services for emergency communications systems, grant recipients 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 P25 accredited technical standards for LMR and the *P25 Steering Committee Approved List of Accredited Technical Standards* • Select P25 Compliance Assessment Program (P25 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) • Avoid non-standard and proprietary features, but if necessary, ensure features are identified and understand impacts on operability and interoperability • Provide written justification for non-compliant P25 purchases
Public Safety Broadband	• Seek guidance from the FirstNet Authority on how to best incorporate broadband communications into a public safety entity's communications ecosystem • Provide detailed requirements for integration of agency's computer-aided dispatch, records management, and other systems for wireless access and broadband services • Request to test various equipment and services offered and verify interoperability of PTT voice, data network services, and one-time password or authenticator applications • Obtain comprehensive cost information for equipment and services offered
Alerts, Warnings, and Notifications	• Read the *IPAWS Best Practices* and consult with IPAWS Program Management Office for compatible alert origination software tools • Reference the IPAWS Program Planning Toolkit • Review the IPAWS list of critical capabilities and recommended features of an alert origination software tool • Ensure software tool compliance with the IPAWS CAP Profile and support of a testing environment • Complete the IPAWS Memorandum of Agreement process
911 Systems	• Discover standards through the *NG911 Standards Identification and Review* • Use the NG911 Self-Assessment Tool to determine NG911 maturity state • Consider SAFECOM and NCSWIC NG911 transition guidance for next steps • Select IP-enabled, accredited standards-based 911 equipment and software
Data Exchange and Information Sharing Environment	• 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 SAFECOM/NCSWIC guidance and best practices provided by the *Approach for Developing an Interoperable Information Sharing Framework*

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 general best practices for recipients to use throughout the grant lifecycle. Table 3 provides best practices during the four major phases of the grant:

- Planning grant applications (Pre-Award)
- Reviewing award agreements and funding (Award)
- Implementing grant-funded projects (Post Award)
- Completing federal grant projects (Closeout)

Table 3. Recommendations 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[71] • 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 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 • Complete projects within grant period of performance
Closeout	• Ensure all projects are complete • Maintain and retain data as required by the award terms and conditions • File closeout reports; report on final performance

[71] Stakeholders can also contact their respective CISA Emergency Communications 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 entirely or partially fund emergency communications projects.

Traditional Grant Funding

CISA is charged with coordinating "grant guidelines for the use of homeland security assistance administered by the Department relating to interopeable emergency communications."federal grants funding emergency communications.[72] Through its work with the ECPC Grants Focus Group, CISA identified more than 90 federal grants and loans that fund emergency communications in the past fiscal year.[73] When applying for these funds, grant applicants 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 *SAFECOM Guidance* traditionally covers DHS financial assistance 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 U.S. Department of Agriculture (USDA) Rural Utility Service 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. While loans offer an alternative to traditional grants, applicants 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. Applicants are encouraged to identify additional funding sources, such as rural grants and loans or private and philanthropic grants, and work with eligible entities for those programs to improve communications infrastructure.

Funding and Sustainment Resources

CISA, 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 nonexhaustive list includes educational documents and tools designed for stakeholders, available on the SAFECOM Funding Resources webpage.

- *Funding Mechanisms Guide for Public Safety Communications,* assists public safety agencies in identifying funding sources for emergency communications projects. It highlights strengths, challenges, opportunities, and other considerations for funding sources to help agencies determine if

[72] 6 U.S.C. § 574(a).

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

certain mechanisms are suitable for their community. The guide also provides funding examples from states and localities, showcasing challenges and successes associated with real-world applications.

- *Emergency Communications System Lifecycle Planning Guide* and the *Lifecycle Planning Tool*, aids stakeholders in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually to replace and dispose of system components.
- *Emergency Communications Systems Value Analysis Guide* and the accompanying *Understanding the Value of Public Safety Communications Systems: A Brochure for Elected Officials and Decision-Makers*, assist public safety agencies in evaluating communications systems and equipment for cost-effectiveness and value to its users. Materials describe common system components, including considerations and features required by public safety agencies that are unique to specific roles.
- *Funding and Sustaining LMR: Materials for Decision Makers*, provides an overview of radio systems, including information on their importance to public safety communications, as well as challenges to consider when upgrading systems.
  - *Funding and Sustaining LMR Trio, Part 1: Educating Decision-Makers on LMR Fundamentals*, includes information on basic LMR system components such as simple diagrams, terminology, history, and current usage of LMR technologies by public safety agencies.
  - *Funding and Sustaining LMR Trio, Part 2: 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 the LMR-to-LTE transition, and the need to sustain mission-critical voice through such transitions.
  - *Funding and Sustaining LMR Trio, Part 3: Educating Project and Acquisition Managers on Project 25*, delivers an introduction to standards-based purchasing, and an overview of the P25 standard explaining its importance to public safety interoperability.
  - *Funding and Sustaining LMR Systems Brochure*, serves as a tri-fold handout for state, local, tribal, and territorial government decision-makers, and elected officials to explain the importance of funding and sustaining public safety radio systems.
  - *Promoting the Importance of Funding and Sustaining LMR Action Memorandum*, urges decision-makers to support the funding and sustainment of LMR systems. To help decision-makers justify these purchases, the memorandum summarizes best practices from the LMR Trio and provides a list of resources for more information.
- *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.
- *Contingency Considerations When Facing Reductions in Emergency Communications Budgets*, provides a series of contingency considerations to justify investment in four mission-critical resource categories: personnel, operating costs, equipment, and software.
- *Contingency Planning Guide for Emergency Communications Funding*, provides a comprehensive look at the considerations public safety officials must weigh when planning for or facing budget reductions and recommends actions to take before, during, and after budget cuts.

In addition, public safety agencies may reference materials on the SAFECOM Technology Resources and SAFECOM P25 Resources webpages to inform planning and funding for emergency communications projects.

- *The Funding and the Future of P25* video, provides an overview of the value and advantages of P25 as a long-term investment in a community's public safety. Presented through interviews of emergency communications practitioners and managers nationwide, the six-minute video focuses on the features and comparative costs of P25 standards-based systems versus non-P25 systems, the practical value of P25 technology in public safety operations, and recommendations for funding P25. Looking ahead, the presenters discuss the current states of P25 and LTE broadband technology, emphasizing the durability, transmitting power, one-to-many communication, and emergency push-to-talk features of P25 radios. Their conclusion: P25 and LTE are not exclusive options but likely complementary components of public safety communications in the future.

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
ATIS	Alliance for Telecommunications Industry Solutions, Inc.
AUXCOMM	Auxiliary Communications
AWN	Alerts, Warnings, and Notifications
CAP	Common Alerting Protocol
CAPRAD	Computer Assisted Pre-Coordination Resource and Database
CASM	Communication Assets Survey and Mapping
CDM	Continuous Diagnostics and Mitigation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CJIS	Criminal Justice Information Services
CJI	Criminal Justice Information
CEQR	Council on Environmental Quality Regulations
COLT	Cell on Light Trucks
COML	Communications Unit Leader
COMSEC	Communications Security
COMT	Communications Technician
CONOPS	Concept of Operations
COW	Cell on Wheels
CRD	Compact Rapid Deployables
CSIRT	Computer Security Incident Response Team
CSRIC	Communications Security Reliability and Interoperability Council
CSSI	Console Subsystem Interface
CSSP	Communications Sector-Specific Plan
DE	Distribution Element
DES-OFB	Data Encryption Standard-Output Feedback
DHS	Department of Homeland Security
EAS	Emergency Alert System
ECC	Emergency Communications Center
ECPC	Emergency Communications Preparedness Center

EDXL	Emergency Data eXchange Language
EHP	Environmental Planning and Historic Preservation
EO	Executive Order
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FirstNet Authority	First Responder Network Authority
FY	Fiscal Year
GETS	Government Emergency Telecommunications Service
GFIPM	Global Federated Identity and Privilege Management
GRA	Global Reference Architecture
GSMA	Groupe Speciale Mobile Association
HAVE	Hospital Availability Exchange
HF	High Frequency
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, 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
INCM	Incident Communication Center Manager
INTD	Incident Tactical Dispatcher
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPS	Intrusion Prevention System
IS	Independent Study
ISE	Information Sharing Environment
ISO	International Organization for Standardization
ISSI	Inter Radio Frequency Subsystem Interface
IT	Information Technology
ITS	Intelligent Transportation Service
ITSL	Information Technology Service Unit Leader

ITSS	Information Technology Service Specialist
ITU	International Telecommunication Union
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MFA	Multi-Factor Authentication
MHz	Megahertz
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Advisory Council
NASNA	National Association of State 911 Administrators
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
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Reports
NOFO	Notice of Funding Opportunity
NPSBN	Nationwide Public Safety Broadband Network, or FirstNet
NRI	National Risk Index
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OMA	Open Mobile Alliance
OMB	Office of Management and Budget
P25	Project 25
P25 CAP	P25 Compliance Assessment Program
PACE	Primary, Alternate, Contingent, and Emergency
PMO	Project Management Office
POETE	Planning, Organization, Equipment, Training, and Exercises
PSAP	Public Safety Answering Point
PSCR	Public Safety Communications Research

PSHSB	Public Safety & Homeland Security Bureau
PTIG	Project 25 Technology Interest Group
RADO	Radio Operator
RAN	Radio Access Network
RECCWG	Regional Emergency Communications Coordination Working Group
RECP	Regional Emergency Communications Plans
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposal
RM	Resource Messaging
SAA	State Administrative Agency
SAME	Specific Area Message Encoding
SCIP	Statewide Communication Interoperability Plan
SDO	Standard Development Organization
SHARES	SHAred RESources High Frequency Radio Program
SIEC	State Interoperability Executive Committee
SIGB	Statewide Interoperability Governing Body
SLIGP	State and Local Implementation Grant Program
SOP	Standard Operating Procedure
SOW	Statement of Work
SPR	Stakeholder Preparedness Review
SWIC	Statewide Interoperability Coordinator
TDoS	Telephony 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
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
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Service
XML	Extensible Markup Language

Appendix B – Technology and Equipment Standards and Resources

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

How to Use this Appendix

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

System Lifecycle Planning

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

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

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

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

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

Cybersecurity

Grant recipients should implement the *NIST Cybersecurity Framework* and take advantage of existing cybersecurity standards, guidance, tools, and resources

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

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

Cybersecurity Framework

The National Institute of Standards and Technology (NIST) developed the *Cybersecurity Framework* as a flexible and voluntary risk-based approach that outlines techniques to reduce cybersecurity risk. The new 2.0 edition (released in February 2024) is designed for all audiences, industry sectors, and organization types—regardless of their degree of cybersecurity sophistication. 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. In addition to NIST materials, sector-specific Cybersecurity Framework guidance is available from CISA.

The NIST Cybersecurity Framework establishes six functions to integrate cybersecurity into mission functions and operations, including: 1) ***govern*** the organization's cybersecurity risk management strategy, expectations, and policy; 2) ***identify***, evaluate, and prioritize risks; 3) ***protect*** against identified risks; 4) ***detect*** attacks and compromises to the network as they arise; 5) ***respond*** with actions to cybersecurity incident; and 6) ***recover*** assets and operations affected to ensure the resiliency and continuity of communications. CISA'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.[74]

There is considerable cybersecurity guidance available from government, industry, and academic organizations and a multitude of standards development organizations (SDOs) that contribute to technical standards and best practices. Organizations managing critical infrastructure will continue to have unique risks—different threats, different vulnerabilities, and different risk tolerances—and how they implement the standards and guidance available will vary. There is currently no one-size-fits-all network cybersecurity solution. Table B-2 lists some of the potentially applicable standards for cybersecurity that recipients should leverage as they identify and select the standards that fit their system and mission needs. Table B-3 lists

[74] Suggested resource includes the *Emergency Services Sector Cybersecurity Framework Implementation Guidance*.

cybersecurity resources for additional information. While these lists are not exhaustive, they include some of the more comprehensive guidance for the public safety community.

Table B-2. Cybersecurity Standards

Organizations	Standards
Third Generation Partnership Project (3GPP) Security Standards	3GPP's security working group, SA3, is continuously updating security standards associated with prevalent technologies. 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.
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. Also, outputs of the Alliance for Telecommunications Industry Solutions (ATIS) Emergency Services Interconnection Forum, Next Generation Interconnection Interoperability Forum, and Wireless Technologies and Systems Committee are important to the public safety community.
Criminal Justice Information Services (CJIS) Security Policy	CJIS standards contain information security requirements, guidelines, and agreements reflecting the will of law enforcement agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information.
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. Public safety mapping and communications site available.
Federal Information Processing Standards (FIPS)	FIPS establishes the minimum-security requirements for federal information systems.
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.
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.
Institute of Electrical and Electronics Engineers (IEEE)	IEEE produces sector-specific security standards, as well as industry guidance. Of interest to networks may be the 802, 1363, and 1619 series, as well as C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems.
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.
Internet Engineering Task Force (IETF)	IETF Working Groups are the primary mechanism for development of IETF standards. IETF Working Groups currently have more than 600 standards regarding security mechanisms, integrity mechanisms, network layer security, transport layer security, application layer security, encryption algorithms, key management, secure messaging, etc.

Organizations	Standards
National Fire Protection Association 1221/1225	A standard for the installation, maintenance, and use of emergency services communications systems, including cybersecurity considerations.
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. In particular, NIST 800-53r5 covers Cybersecurity and Privacy controls and NIST 800-63-4 covers requirements for implementing digital identity solutions.
North American Electric Reliability Corporation (NERC) Reliability Standards	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.
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.

Table B-3. Cybersecurity Resources

Organizations	Resources
Committee on National Security Systems	• Committee on National Security Systems Policies
Department of Homeland Security (DHS)	• CISA's Public Safety Communications and Cyber Resiliency Toolkit • CISA Central • CISA Cyber Essentials Toolkit • CISA Learning • CISA Transition to NG911 Resources • CISA 911 Cybersecurity Resource Hub for Emergence Communications Centers • CISA Cybersecurity Training and Exercises • CISA Emergency Services Sector Cybersecurity Framework Implementation Guidance • CISA "First 48": What to Expect When a Cyber Incident Occurs • CISA Guide to Getting Started with a Cyber Risk Assessment • CISA Resources for State, Local, Tribal, and Territorial (SLTT) Governments • CISA Stop Ransomware / Public Safety Emergency Communications Resources • Cybersecurity Incident & Vulnerability Response Playbooks • Cyber Resiliency Resources for Public Safety Fact Sheet • ESS Cybersecurity Framework Implementation Guidance – 2023 • National Cyber Incident Response Plan • National Infrastructure Protection Plan • Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure – 2024 • Public Safety Cybersecurity
Department of Energy	• Energy Sector Cybersecurity Capability Maturity Model (C2M2) Program

Organizations	Resources
Executive Orders (EO) and President Directives	• EO 13636: Improving Critical Infrastructure Cybersecurity • EO 13231: Critical Infrastructure Protection in the Information Age • EO 13618: Assignment of National Security and Emergency Preparedness Communications Functions • Executive Office of the President, Presidential Policy Directive 21 • EO 13407: Public Alert and Warning System • EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure • EO 14028: Improving the Nation's Cybersecurity
Federal Bureau of Investigation	• Cyber Crime • Federal Bureau of Investigation Internet Crime Complaint Center Industry Alerts
Federal Communications Commission	• Communications Security, Reliability and Interoperability Council (CSRIC) • Task Force on Optimal PSAP Architecture (TFOPA) • Cyber Security Planning Guide
Federal Emergency Management Agency	• Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC) • Cybersecurity Gap Analysis, FEMA National Cyber Resilient Architecture, and Training resources
Government Accountability Office	• U.S. Government Accountability Office, Cybersecurity
National Institute of Standards and Technology	• Cybersecurity Framework 2.0 • Internal/Interagency Reports (NISTIRs) • National Initiative for Cybersecurity Education (NICE) • NICE Cybersecurity Workforce Framework • Assessing Security and Privacy Controls in Information Systems and Organizations • Digital Identity Guidelines
Various Industry and Associations	• ATIS Industry Best Practices • Association of Public-Safety Officials, International (APCO), APCO Cybersecurity, and Cybersecurity Resources, including *APCO Cybersecurity Guide for Public Safety Communications Professionals* and *APCO Introductory Guide to Cybersecurity for PSAPs* • ISACA COBIT 2019 Framework • ITU Security Standards Roadmap • Center for Internet Studies (CIS) Critical Security Controls (CSC), available through the Multi-State Information Sharing and Analysis Center, as well as hardened images • National Association of State Chief Information Officers (NASCIO) Cybersecurity Resources • NENA, including the ANSI-approved NENA Security for Next Generation 9-1-1 Standard (NG-SEC), NENA-STA-040.2-2024. The standard establishes the minimal guidelines and requirements for the protection of NG9-1-1 assets or elements within a changing business environment.

Continuity and Resilience

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

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

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

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

Table B-4. Continuity and Resilience Resources

Resource	Description
FEMA National Continuity Programs	National Continuity Programs highlight the national policy and guidance for continuity of operations initiatives. They provide guidance and assistance to support continuity preparedness for federal departments and agencies; state, local, tribal, and territorial government jurisdictions; and private sector organizations.
CISA Shields Ready	Shields Ready campaign is designed to help all critical infrastructure stakeholders to take action to enhance security and resilience—from industry and businesses to government entities at all levels, and even individuals by providing recommendations, products, and resources to increase individual and collective resilience for different risk contexts and conditions.
CISA Regional Resiliency Assessment Program	The Regional Resiliency Assessment Program is a cooperative assessment of specific critical infrastructure within a designated geographic area. DHS works with selected areas each year to conduct a regional analysis of surrounding infrastructure and address a range of resilience issues that could have significant regional or national consequences if disrupted.
CISA Ten Keys to Obtaining a Resilient Local Access Network	This document introduces resiliency concepts and provides ten keys to obtaining and maintaining resiliency in a local access network, such as knowing the exact network infrastructure in the local loop, interfacing with commercial service providers, and properly maintaining alternative path solutions. CISA developed these ten fundamental steps, supported by descriptive text and visually appealing graphics, as recommendations to help organizations maintain critical communications in emergency situations.
CISA Public Safety Communications Resiliency Self-Assessment Guidebook	This document provides a self-assessment methodology for public safety entities to identify and address potential points of failure in their communication networks by evaluating the local access networks of their primary and alternate operating facilities. The methodology describes the process of gathering data on network infrastructure, creating logical and physical network maps, and choosing resiliency solutions based on the network maps. DHS also developed a Resiliency Fact Sheet to understand communications continuity planning and offer resources to assist entities.
CISA Priority Services Programs	Priority Services Programs, including the Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority, support national leadership; federal, state, local, tribal, and territorial governments; first responders; and other authorized national security and emergency preparedness users. They are intended to be used in an emergency or crisis when data, landline, or wireless networks are congested and the probability of completing a normal transmission or call is reduced.
CISA Electromagnetic Pulse (EMP) Guidance	The EMP Protection and Resilience Guidelines for Critical Infrastructure and Equipment provides guidelines to assist federal, state, and local officials and critical infrastructure owners and operators to protect mission essential equipment against EMP threats. There are four EMP Protection Levels defined. These levels were initially developed at the request of the federal Continuity Communications Managers Group but are applicable to any organization that desires to protect its electronics and critical infrastructures.
Infrastructure Obstructions to Radio Propagation	This document provides an overview of obstructions and interferences to radio frequency resources, including both active and passive sources. In addition, it includes a series of example planning approaches that agencies have taken to prevent or mitigate obstructions.
Public Safety Communications and Cyber Resiliency Toolkit	This toolkit assists public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats. Through an interactive graphic, users can explore topic specific systems-based resources and learn more about key threats to communications and cyber resiliency.

Resource	Description
Public Safety Communications Dependencies on Non-Agency Infrastructure and Services	This white paper provides high-level insights on non-agency communications infrastructure for system administrators, public safety decision-makers, and other stakeholders involved in public safety communications planning or implementation. While not a comprehensive guide, this document equips stakeholders with real-word examples of these dependencies, recommendations for ensuring resiliency and continuity of operations, and supplemental resources.
Radio Frequency Interference Best Practices Guidebook	This document provides stakeholders with an overview of RF interference concepts, threats, and mitigation initiatives. Applicants can review this guidebook to understand ongoing efforts related to awareness, preparation, mitigation, and current laws pertaining to RF interference. The document also provides best practices on how to recognize, respond to, report, and resolve RF interference incidents.
Resilient Power Best Practices Fact Sheet	This document summarizes recommendations from the CISA Resilient Power Working Group, consisting of federal, state, local, tribal, and territorial stakeholders, non-profits, and private industry. These critical communications infrastructure best practices should be part of a comprehensive, risk-informed Business Continuity and Continuity of Operations plans, developed per FEMA guidance.
CISA Infrastructure Dependency Primer	This tool is a supplement to the Infrastructure Resilience Planning Framework and is intended to help state and local planners better understand how infrastructure dependencies can impact risk and resilience in their community and incorporate that knowledge into planning activities.

Land Mobile Radio	Grant recipients should purchase digital LMR systems and equipment compliant with the Project 25 (P25) Suite of Standards (Telecommunications Industry Association), and include all needs and requirements, identifying applicable P25 standards and stating their agency requirements for interoperability in any SOW or acquisition documents
	Recipients should purchase P25 compliant systems and equipment that has been assessed as compliant in accordance with the P25 Compliance Assessment Program, or approved test procedures of the P25 standards in the absence of completed P25 Compliance Assessment Program testing
	Recipients are strongly encouraged to implement or transition to comprehensive Advanced Encryption Standard (AES) 256-bit encryption on all LMR systems. Use of proprietary/non-standard encryption, privacy options (e.g., ADP, Encryption Lite, ARC4), or deprecated encryption (i.e., Data Encryption Standard [DES] and all derivatives) is not an acceptable use of federal grant funding as these algorithms have been compromised, deprecated, and offer little protection
	Recipients should ensure all P25 eligible equipment, features, functions, and capabilities selected are P25 compliant and are tested to ensure interoperability, to include new equipment and upgrades
	When purchasing interoperability equipment, services, and gateway devices to provide connectivity between LMR systems, those devices should, at a minimum, be implemented using P25 compliant wireline interfaces (e.g., ISSI, CSSI, DFSI)

LMR systems are terrestrially-based, wireless, narrowband communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works/public service entities, and the military in non-tactical environments, to support voice and low-speed data communications. These systems are designed to meet public safety's unique mission and critical voice requirements and support time-sensitive, lifesaving tasks, including sub-second voice call-setup, group calling capabilities, high-quality audio, and priority access to the end-user. Because LMR systems implemented by the public safety community support responders' safety and lifesaving operations, they are designed and implemented to achieve the highest levels of availability, 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 digital trunked systems incorporating IP networking, digital protocols, and trunked features. These enhancements have improved the interoperability, spectral efficiency, security, reliability, availability, redundancy, and functionality of voice and low-speed data communications.

The public safety community is following a multi-path approach to develop, establish, and maintain critical communications capabilities. To improve interoperability across investments, grant recipients are strongly encouraged to ensure digital voice systems and equipment purchased with federal grant funds are compliant with the Project 25 (P25) Suite of Standards, unless otherwise noted in a program's grant guidance.[75] Recipients should ensure all new and upgraded P25 eligible equipment, features, functions, and capabilities

[75] Applicants should read grant guidance carefully to ensure compliance with standards, allowable cost, documentation, reporting, and audit requirements. If interested in using federal funds to purchase equipment that does not align with P25 standards or does not appear on the approved equipment list, the applicant should consult with DHS and their own legal advisor 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 accredited technical 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 accredited technical standards-based equipment.

selected for procurement are verifiably P25 compliant and interoperable. When federal grant funds are used to purchase P25 LMR equipment and systems that contain non-standard features or capabilities while a comparable P25 feature or capability is available, recipients must ensure the standards-based feature or capability is also purchased to ensure interoperability. For more information on P25, contact the P25 Steering Committee at Project25SC@cisa.dhs.gov.

Grant recipients should purchase P25 compliant systems and equipment that have been assessed in accordance with the P25 Compliance Assessment Program (P25 CAP). P25 accredited technical standards provide many technical specifications designed to ensure equipment is interoperable regardless of manufacturer. Recipients should obtain documented evidence of P25 compliance from the manufacturer that the equipment has been tested and passed all the applicable, published, normative P25 compliance assessment test procedures for performance, conformance, and interoperability as defined in the latest P25 Compliance Assessment Bulletins for testing requirements. If such testing and compliance documentation for-to-be acquired applicable equipment is not available through the P25 CAP or there is an absence of applicable testing in the P25 CAP, recipients should obtain documented evidence from the manufacturer stating that all applicable tests were conducted in accordance with the published test procedures in the P25 Suite of Standards and successfully passed.[76] In the absence of applicable P25 testing procedures, agencies should work with the providing manufacturer/vendor to ensure that procured equipment or services meet stated requirements and are interoperable with the procuring agency’s known interoperability partners. Contact the P25 CAP at P25CAP@hq.dhs.gov for additional guidance.

Encryption

Recipients using DHS funds to purchase encryption for new or existing communications equipment shall ensure encryption capabilities are compliant with the published P25 Block Encryption Protocol Standard. Recipients investing in any encryption capability must also implement the AES 256-bit Encryption Algorithm as specified in the P25 Block Encryption Protocol. In this context, “must implement” means that the LMR equipment (i.e., portable, mobile radios, console equipment) to be acquired is properly provisioned and equipped with all necessary firmware, hardware, and necessary services to receive encryption key(s) from a Key Management Facility or a Key Fill Device. Acquiring equipment that is “capable” but must undergo future upgrades to add a cryptographic module, features, firmware, or software is inconsistent with the requirement.

References to the current version of the P25 Block Encryption Protocol, ANSI/TIA-102.AAAD should be included in all procurement documents, along with specific agency requirements for primary, alternate, contingency, and emergency communications systems or interoperability systems/capabilities where applicable.

AES is endorsed by NIST and is the only encryption algorith that complies with the P25 standards. While the P25 accredited technical standards continue to include references to the Data Encryption Standard-Output Feedback (DES-OFB), it is considered deprecated, obsolete, and provides little to no actual information protection.

[76] Regardless of the status and availability of P25 CAP testing documentation, grant recipients should include comprehensive acceptance test plan(s) and testing criteria of stated requirements in their procurement and contractual documents to ensure that the required and expected interoperability of features, functions, and services has been provided, especially in multi-manufacturer/vendor implementation environments. The manufacturer/vendor should verify (as part of formal systems acceptance processes) the equipment or services are P25 standards compliant and interoperable with other equipment, features, functions, and capabilities.

It is imperative that entities continue to transition to a common AES 256-bit only environment to ensure secure encrypted interoperable communications with public safety partners at all levels of government. While most federal agencies have transitioned to AES encryption, some state, local, tribal, and territorial agencies continue to use DES, DES derivatives, or other manufacturer proprietary/non-standard encryption algorithms as their primary means of encryption.

However, the continued use of DES and its derivatives enables known vulnerabilities in LMR encryption. NIST, which approved the use of DES in 1976, withdrew *Federal Information Processing Standard (FIPS)-46, Data Encryption Standard* on May 19, 2005, citing the weakness and repeated compromise of DES and the availability of the current federal standard specified in *FIPS-197, Advanced Encryption Standard*. DES has since been deprecated in P25 standards. As a result, current federal laws and regulations mandate that federal agencies are only permitted to use NIST approved AES 256-bit encryption.[77] For more information, see CISA's *Transition to AES*.[78]

Recipients should not use federal grant funds to purchase non-standard, deprecated encryption features (e.g., 40/56-bit encryption, proprietary/manufacturer privacy solutions, DES or any DES derivatives). If applicants purchase or acquire encryption capabilities other than the NIST approved AES 256-bit encryption for new or existing equipment, recipients must ensure AES 256-bit encryption is purchased for secure communications and secure interoperability with other emergency responders at all levels of government. Agencies currently using DES or DES derivatives should migrate to AES for all encryption as soon as possible. The continued use of DES, its derivatives, manufacturers' privacy features, or other non-standard encryption algorithms for any LMR encryption is strongly discouraged and presents substantial risks of compromised communications and the potential breach of sensitive information.

Agencies acquiring encryption capabilities are strongly encouraged to only procure subscriber equipment that supports multi-key operations and capabilities. This allows multiple encryption keys to be stored within the subscriber unit's cryptographic module facilitating the use of different encryption keys for channels or talkgroups. Multikey capabilities also permit more than one Key Management Facility or Key Fill Device to provide encryption keys to subscriber devices. Single key capable devices only permit the use of a single encryption key. Agencies should also consider how they will accomplish encryption key management requirements to periodically add or modify deployed keys.

Lastly, agencies considering encryption capabilities should also evaluate the potential addition of P25 Link Layer Authentication (LLA) for trunked networks and Link Layer Encryption (LLE) to their encryption plan. LLE is nearing technical standards development completion and potential product availability in the next several years.

Interconnecting Systems

When purchasing P25 interoperability equipment, services, and devices to provide connectivity between LMR systems, those devices should, at a minimum, implement the P25 wireline interfaces, such as the Inter Radio Frequency Subsystem Interface (ISSI), Console Subsystem Interface (CSSI), or Digital Fixed Station Interface (DFSI).

[77] The 2002 Federal Information Security Management Act, Public Law 107-347, and the 2014 Federal Information Systems Modernization Act, Public Law 113-283, prohibits the use of any other encryption algorithm by federal entities. While these statutes permit only NIST approved AES encryption use by federal entities, such prohibitions do not directly apply to SLTT agencies. However, SLTT agencies desiring to maintain encrypted interoperable communications with federal agencies should transition to AES 256-bit encryption.

[78] CISA's *Transition to Advanced Encryption Standard* document is available at: cisa.gov/sites/default/files/2023-10/23_0918_fpic_AES-Transition-WhitePaper_Final_508C_23_1023.pdf.

There are potential interoperability issues of P25 system features, functions and services afforded by these interfaces when implementing ISSI/CSSI/DFSI, especially when using various system manufacturers as there are implementation differences driven by each manufacturer's interpretation of the technical standards. These implementation differences may manifest in the lack of interoperability of current P25 system features, functions, and services supported by and through these interfaces. Therefore, it is imperative that agencies implementing ISSI, CSSI, or DFSI create comprehensive needs and requirements documentation specifically detailing which P25 features, functions, and services are required, and the expected behaviors of the connected systems supported by the ISSI, CSSI, or DFSI.

While baseline P25 accredited technical standards for ISSI/CSSI/DFSI connections exist, they remain under development and revision. Due to the limited availability of completed technical standards and differing manufacturer's features and functionality implementation practices, public safety agencies should consider the planning and technical complexities associated with the implementation of ISSI/CSSI/DFSI capabilities to connect RF-subsystems (RFSS) from the same or dissimilar LMR suppliers/manufacturers. As such, grant applicants should:

- Ensure that existing operability and interoperability between RFSS/networks remain intact and operational during and after ISSI/CSSI implementation;
- Identify explicit requirements of features, functionalities, and capabilities that the ISSI/CSSI/DFSI connections will support to a same or dissimilar manufacturer's RFSS/systems, including interoperability requirements, in any SOW, acquisition documents, or contracts;
- Require the prospective vendor/manufacturer to demonstrate their ability and acceptance to provide these explicit features, functionalities, and capability requirements for ISSI/CSSI/DFSI implementations, regardless of which manufacturer's ISSI/CSSI/DFSI and RFSS/networks are in place, in the appropriate purchasing agreements or contracts;
- Confirm the selected supplier/manufacturer develops and executes a comprehensive acceptance test plan that validates P25 accredited standards compliance, as well as successful operability and interoperability of features, functions, and capabilities on each side of the ISSI/CSSI/DFSI connection(s), consistent with procurement and acquisition requirements, and compliance with agreed upon performance, applicable technical standards, passage of available standards-based testing, and expectations of operations amongst ISSI/CSSI/DFSI connected RFSS/networks;
- Submit evidence to the DHS, if required, documenting successful P25 CAP testing (e.g., P25 product Summary Test Reports available on the P25 CAP website), certifying compliance with applicable accredited technical standards, as well as evidence of effective operability and interoperability of features, functions, and capabilities with all ISSI partners.

Interconnecting LMR and Broadband Networks

Applicants may also be interested in using DHS grant funds to enable interoperability between existing LMR and long-term evolution (LTE) or 5G/6G broadband networks. Note, TIA/ATIS P25 accredited technical standards for interconnecting LMR to LTE/5G/6G systems remain under development. While the 3GPP accredited standards exist, the TIA/ATIS P25 accredited standards remain a work in progress. Notwithstanding, agencies should pursue solutions that are 3GPP standards compliant and interoperable. Agencies should also thoroughly investigate prospective vendor plans for supporting changes to their product offerings when the TIA/ATIS P25 standards for interconnecting and internetworking P25 to LTE/5G/6G are completed.

Agencies should be aware of the multiple proprietary solutions offered by vendors/manufacturers that may provide acceptable LMR to LTE/5G/6G voice service integrations. However, while potentially achieving adequate LMR to LTE/5G/6G voice interoperability, these proprietary solutions may not be interoperable amongst themselves or with a broadband provider's network level Push-to-Talk (PTT) voice service, thus creating an LTE/5G/6G interoperability issue. Additionally, the indiscriminate, non-planned use of some LTE/5G/6G to LMR Over-the-Top (OTT) PTT solutions has proven to be potentially detrimental to the hosting LMR systems and created significant operability issues due to site loading issues on the host system infrastructure. Investing in solutions that are not based on open standards is a misuse of federal funds, as additional solutions may be needed to restore or provide required interoperability among participating jurisdictions.

Considering the numerous PTT OTT voice solutions and the cautions regarding the lack of interoperability of these PTT services and applications, agencies should fully explore (and test) PTT solutions with potential providers while ensuring the agency's requirements for LMR to broadband voice capabilities are met. Agencies should work closely with the federal granting agency, broadband providers, and application suppliers to ensure that grant-funded systems and equipment will be compatible and interoperable with current and future solutions. Agencies should also consider the broadband provider, PTT services, or OTT applications that current and future interoperability partners have selected as interoperability across providers, services, and applications may not be available.

Grant applicants should consult DHS *before* submitting requests for ISSI/CSSI and LMR to LTE/5G/6G broadband-related project investments to determine whether certain costs are allowed.

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

Table B-5. Land Mobile Radio Standards and Resources

Organizations	Standards and Resources
P25 Compliance Assessment Program	P25 CAP is a partnership of DHS, 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 standards with published results. It publishes Compliance Assessment Bulletins on policy, testing, and reporting requirements, and an approved equipment list that may be eligible for grants.
P25 Steering Committee	P25 Steering Committee is the governing authority of P25 and the sole authority for approving standards proposals, telecommunications system bulletins, and white papers. It works closely with manufacturers to develop and maintain the P25 Suite of Standards that best serves the continually evolving needs of the public safety community. The committee recently produced the *Statement of P25 User Needs*, which provides high-level explanations of system architecture, features, and functions as defined in P25 standards.
Telecommunicat-ions Industry Association	TIA is accredited by the American National Standards Institute and responsible for publishing the P25 Suite of Standards, approved by the P25 Steering Committee. To date, it 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.
SAFECOM P25 Resources	This webpage contains multiple P25 and LMR encryption resources, including the *Operational Best Practices for Encryption Key Management*, *P25 ISSI and CSSI Primer*, and *Best Practices for Planning and Implementation of P25 ISSI and CSSI, Volumes I and II*.
911 Program Office	The 911 Program Office provides several resources on LMR standards for interconnecting NG911 systems and broadband technologies. These include the NG911 Interstate Playbook, which provides best practices, guidance, and considerations on PSAP interconnectivity with NG911, as well as the 911 Program Office's NG911/Public Safety Broadband Network Interconnection resource page.

Public Safety Broadband

Applicants interested in investing federal funds in broadband-related infrastructure projects should consult DHS to understand all requirements and restrictions impacting broadband investments

Grant recipients should consult with any applicable governing bodies and the FirstNet Authority to ensure the project does not conflict with network deployment efforts

Recipients may be able to use grant funds for the implementation of alternative broadband technologies and the deployment of fiber optic backhaul networks in rural and unserved areas

Applicants investing in broadband technologies should be aware that the federal government is overseeing the operations and maintenance of the Nationwide Public Safety Broadband Network (NPSBN). The First Responder Network Authority's (FirstNet Authority) mission is to ensure the building, deployment, and ongoing operation of the NPSBN to provide LTE-based broadband and 5G services and applications to public safety entities. The network is a single, nationwide network architecture consisting of a secure, redundant evolved packet core network (EPC), transport backhaul, and radio access networks (RANs) in the 50 states, five territories, and the District of Columbia.

Applicants should coordinate with the FirstNet Authority in advance of any strategic acquisition of LTE equipment to ensure understanding of all requirements and restrictions impacting broadband investments and that purchases support future service choices. Applicants should also monitor federal actions affecting broadband investments and continue to stay abreast of advancements in the NPSBN/FirstNet and the commercial broadband industry that may have positive benefits for public safety use of available networks and services such as:

- Leveraging broadband devices including, but not limited to smartphones, feature phones, tablets, wearables, laptops, ruggedized smartphones, ruggedized tablets, USB modems/dongles, in-vehicle routers, and Internet of Things devices;
- Utilizing broadband networks for LMR coverage extension beyond a jurisdiction's dedicated LMR coverage area;
- Employing agency-owned and managed broadband deployable equipment, enabling public safety agencies to own and provide coverage expansion or capacity enhancement equipment within their jurisdiction;
- Using broadband device accessories that enable efficient and safe public safety operations such as headsets, belt clips, earpieces, remote Bluetooth sensors, and ruggedized cases;
- Installing standards-based equipment to provide internetworking between LTE/5G/6G and existing LMR systems;
- Installing FirstNet SIM/UICC devices to allow public safety users to update existing devices, "Bring Your Own Device" plans, and new devices to operate on public safety broadband prioritized services;
- Securing 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; and
- Developing in-building coverage solutions that help users maintain connections to their mission critical networks and services.

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

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

Table B-6. Broadband Technology Standards and Resources

Organizations	Standards and Resources
FirstNet Authority	The Middle Class Tax Relief and Job Creation Act of 2012 created the FirstNet Authority as an independent authority within the National Telecommunications and Information Administration to provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety. In establishing requirements for the NPSBN and providing 20 MHz of the upper 700 MHz spectrum to the FirstNet Authority, Congress directed the Authority to ensure the building, operation, and maintenance of a wireless, interoperable Nationwide Public Safety Broadband Network (NPSBN/FirstNet) based on a single national network architecture. The Authority holds the single nationwide FCC license for the 20 MHz of combined Public Safety Broadband Spectrum (758-768 MHz and 788-798 MHz), commonly referred to as Band 14. The FirstNet Authority license also incorporates two one-MHz guard bands at 769 and 799 MHz. Subscription to the NPSBN and use of approved NPSBN devices enables prioritized access to Band 14 spectrum for public safety entities.
3GPP	3GPP is the SDO responsible for development and maintenance of LTE and 5G specifications, though various standards from TIA, ATIS, the Groupe Speciale Mobile Association (GSMA), and the Open Mobile Alliance (OMA) also contribute to broadband functionality and interoperability.
IEEE	The 802.11a, 802.11b/g/n, and 802.11ac wireless standards are collectively known as Wi-Fi technologies and developed and maintained by IEEE. The Official IEEE 802.11 Working Group Project Timelines provides status of each networking standard under development, and a link to each effort. IEEE also maintains the WiMAX family of 802.16 standards.
Open Geospatial Consortium (OGC)	OGC is an international non-profit organization committed to making quality open standards for the global geospatial community. These standards are made through a consensus process and are freely available for anyone to use to improve sharing of the world's geospatial data.

Alerts, Warnings, and Notifications

Grant recipients using funds to cover costs associated with AWN systems should:

- Establish strong governance and engage in collaboration with existing AWN stakeholders
- Ensure well-documented and field-tested plans, policies, and procedures, are executed, evaluated for potential gaps, and adapted to evolving AWN capabilities
- Invest in secure and resilient AWN solutions, and incorporate safeguards to ensure the accuracy of messaging
- Invest in solutions that enable comprehensive, targeted, specific, and transparent messaging, while minimizing issuance and dissemination delays
- Select software or equipment that also supports regional operable and interoperable solutions

Grant recipients should select IPAWS-compatible software that meets the IPAWS minimum interface standards and recommended features[79]

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

FEMA, in accordance with Executive Order 13407, developed IPAWS to ensure that under all conditions the President of the United States can alert and warn the public via the National Public Warning System, a component of IPAWS. In addition, federal, state, local, tribal, and territorial authorities can utilize IPAWS to issue alerts, warnings, and notifications within their jurisdictions. IPAWS improves public safety notification capabilities by allowing authorized Alerting Authorities to deliver AWNs simultaneously through multiple communications pathways, reaching as many people in the impacted area as possible to save lives and protect property. These communication pathways include:

- Emergency Alert System (EAS) used by authorized Alerting Authorities to send detailed warnings via broadcast, cable, satellite, and wireline radio and television channels;
- Wireless Emergency Alerts (WEA) used by authorized Alerting Authorities to geographically target alert messages to mobile devices, generally using cellular broadcast technology;
- National Weather Service Dissemination Systems, including the Weather Radio;
- Unique Alerting Systems, such as siren systems, digital signage, and wall beacons, that have permission to retrieve alerts directly from IPAWS and deliver the alerts to their customer base; and
- Future Systems, including computer gaming systems, Internet search engines, social sharing websites, wireless device applications, smart home technologies, and others that are or could use IPAWS.

To access IPAWS, grant recipients should select equipment and applications that adhere to both the CAP and IPAWS CAP Profile standards, as well as meet the IPAWS minimum critical capabilities. Alert, warning, and notification software and equipment is developed, produced, and distributed by various vendors. While the federal government does not endorse any specific vendor, particular software, or equipment, grant recipients should confirm vendors meet IPAWS compatibility, provide training and support services, use basic security measures (e.g., firewalls, anti-virus tools, anti-spyware tools), implement strong access controls requiring authentication of users, and connect to the IPAWS Technical Support Services environment. In addition,

[79] Contact the IPAWS Program Office (ipaws@fema.dhs.gov) for minimum interface standards and recommended features.

recipients should also consider factors affecting continuity of operations, such as support of remote employees, mobile alerting capabilities, and contingent operations in disruptive circumstances.

To maintain AWN issuance proficiencies, agencies sending alerts should conduct trainings, exercises, and tests of systems on a regular basis. Lessons observed from these activities and incidents should be evaluated, documented, and incorporated into future operations. Alerting Authorities are encouraged to pose any questions about WEA delivery to wireless providers serving their area and to report the results of WEA trainings, exercises, and tests to the Federal Communications Commission's Public Safety and Homeland Security Bureau at WEA@fcc.gov. Alerting Authorities should also work to minimize issuance delays, from the point of a hazard's detection to dissemination, by creating message templates, expediting information sharing, identifying and establishing triggers, and avoiding ad-hoc decision making.

For continued access to IPAWS, and to increase user proficiency and reduce alerting errors, the IPAWS Program Management Office requires authorized Alerting Authorities to demonstrate their ability to compose and send a message through the IPAWS-OPEN system at regular intervals. Such demonstration must be performed monthly through generation of a successful message sent to the IPAWS-OPEN Technical Support Services Facility.

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

Table B-7. AWN Standards and Resources

Organizations	Standards and Resources
Common Alerting Protocol (CAP)	The CAP standard is an open, non-proprietary digital format for exchanging emergency alerts that was developed by Organization for the Advancement of Structured Information Standards (OASIS). CAP allows a consistent alert message to be disseminated simultaneously over many different dissemination mechanisms. The CAP format is compatible with emerging technologies, such as web services, as well as existing formats including the Specific Area Message Encoding used for the Weather Radio and the EAS, while offering enhanced capabilities including images, maps, and video.
OASIS	FEMA worked with OASIS to develop a standardized international technical data profile that defines a specific way of using the standard for the purposes of IPAWS. The CAP standard and supplemental IPAWS CAP Profile ensure compatibility with existing warning systems: oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#tc-tools.
FEMA Integrated Public Alert and Warning System (IPAWS)	The IPAWS Program Management Office (PMO) does not endorse any specific vendor, piece of software, or equipment. The IPAWS Technical Support Services Facility can provide demonstrations of alerting software by contacting the IPAWS PMO at ipaws@fema.dhs.gov.
Public Safety Communications Ten Keys to Improving Emergency Alerts, Warnings & Notifications	This document provides organizations a series of governance, coordination, planning, cybersecurity, and resiliency best practices to help ensure the successful implementation of their emergency AWN systems and programs. Government and nongovernment emergency managers, alert originators, system administrators, system operators, and managers can leverage this foundational guidance to deliver timely and actionable messaging during the critical moments of an incident when coordinated communications—down to the second—can save lives.
Essentials of Alerts, Warnings, and Notifications	Developed with SAFECOM and NCSWIC, this document provides an overview of AWN fundamentals and emerging trends. Applicants can review this guidance for future considerations, next steps, and examples of successful AWN system projects.

911 Systems

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

- Discover standards through the NG911 Standards Identification and Review
- Use the NG911 Self-Assessment Tool to determine NG911 maturity state
- Consider SAFECOM and NCSWIC NG911 transition guidance for next steps
- Select Internet Protocol (IP)-enabled, standards-based 911 equipment and software

The National 911 Program, administrated by the Department of Transportation National Highway Traffic Safety Administration (NHTSA), provides federal leadership and coordination in supporting and promoting optimal 911 services. This federal home for 911 plays a critical role by coordinating federal efforts that support 911 services in emergency communication centers (ECCs)/Public Safety Answering Points (PSAPs) across the nation

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

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

Table B-8. NG911 Resources

Resource	Description
National 911 Program Office	The National 911 Program also provides the 911 community with a collection of documents, website links and other resources generated by both the program and other industry experts. These vetted resources address topics including emerging emergency communications technologies, wireless deployment, E911 location accuracy, cybersecurity, FirstNet, NG911, governance and 911 legislation, and are located in the Document and Tools section of the National 911 Program's website.

Resource	Description
NG911 Maturity State Self-Assessment Tool	This Self-Assessment Tool helps ECC/PSAP administrators and oversight personnel evaluate a system's NG911 maturity state and understand the next steps necessary to continue deployment. It contains a detailed, easy-to-use NG911 readiness checklist that establishes common terminology and identifies key milestones to help 911 call centers understand the multi-year NG911 implementation process. The tool is a downloadable Microsoft Excel file, which ensures that collected results are only shared with the agency completing the assessment. The tool translates the answers from ECC/PSAP personnel into one of six maturity states: Legacy, Foundational, Translational, Intermediate, Jurisdictional End State, or National End State. Adopting and sharing the tool's terminology allows for improved communication—with vendors, industry colleagues, elected officials, and others—at the user's discretion.
National Emergency Number Association (NENA) Security for NG911 Standard	NENA, an ANSI-accredited standards developer, publishes NG911 related standards and best practices related to the network, security, database, and planning. Standards of note for NG911 networks include NENA-STA-010: Detailed Functional and Interface Specification for the NENA i3 Solution; NENA 75-001: NENA Security for NG911 Standard (NG-SEC); NENA 75-502: NG-SEC Audit Checklist; NENA 04-503: Network/System Access Security Information Document, and NENA-INF-015.1-2016: NG911 Security Information Document.
NG911 Standards Identification and Review	Collection of resources from all major standards bodies that address cybersecurity when planning for NG911 deployments.
Cyber Risks to NG911 White Paper	This white paper provides an overview of the cyber risks that NG911 systems may face. It is intended to serve as an informational tool for system administrators to better understand the full scope and range of potential risks, as well as recommend mitigations to these risks. Developed by CISA in conjunction with the Department of Transportation, the document is an introduction to improving the cybersecurity posture of NG911 systems nationwide.
Cyber Risks to NG911: Telephony Denial of Service	This fact sheet familiarizes public safety communications partners with Telephony Denial of Service (TDoS) threats to NG911. The document overviews common TDoS attack vectors, highlights real-world TDoS incidents, and suggests best practices to mitigate TDoS impacts.
NG911 Incident-Related Imagery Impacts 101	This document provides public safety and emergency communications leadership with considerations for addressing incident-related imagery. It also provides topic-specific guidance and available resources.
FCC CSRIC Reports	The Communications Security, Reliability, and Interoperability Council's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.
Geographic Information System (GIS) Lifecycle Best Practices Guide	This guide provides an overview of the GIS lifecycle from planning and implementation to assessing the need to upgrade capabilities. It also highlights best practices for each of the six phases, such as establishing a governance structure, identifying technical requirements for procuring resources, and developing policies and procedures to manage and secure data.
NG911 Interstate Playbook	This resource provides best practices, guidance, and considerations on PSAP transition to NG911. Compiled by state 911 administrators, the playbook's four chapters note new methods of connectivity and information sharing among multiple, separate jurisdictions and states.
NG911/Public Safety Broadband Network Information	This 911 Program Office webpage summarizes current efforts to integrate NG911 and Public Safety Broadband Networks.

Resource	Description
Kari’s Law and RAY BAUM’S Act Compliance	This webpage provides information on Kari’s Law, which ensures anyone can reach a 911 call center when dialing from a multi-line telephone system, as well as the RAY BAUM’S Act, which emphasizes the importance of making dispatchable location information from all 911 calls available to PSAPs. Information includes tools for the 911 Community, such as an overview of legislation, detailed lists of state laws and FCC rules, compliance rules and deadlines, and an interactive checklist towards compliance.
NG911 Procurement Guidance	The National 911 Project has developed NG911 Procurement Guidance for PSAP managers to follow as they upgrade outdated systems. The guidance document assists in the areas of contract negotiation, establishment of scope of work documents, and creation of service for the NG911 system once upgrades are complete. In addition, the document defines a set of important terms used in contract procurements, provides a checklist of considerations while negotiating the Statement of Work, and lists suggestions for ensuring that critical security procedures are established and managed.
The “State of 911” Webinar Series	This webinar series shares information to help states prepare for possible future federal grant funding.
The Successful NG911 Transition: A Case Study of the California Office of Emergency Services	This case study provides insights and guidance directly from the team leading California’s NG911 upgrades at 437 PSAPs. In addition to insights, best practices, and guidance, this case study also provides helpful resources.
The California Statewide NG911 Geographic Information System	This document highlights California’s process of implementing a statewide GIS system. Paired with the *GIS Lifecycle Best Practices Guide for NG911*, it provides users with helpful tips for navigating the GIS lifecycle, including planning, governance, funding, and security considerations.
A Tale of Two Approaches: Mandatory vs. Voluntary Implementations of NG911	This document tackles some common challenges, opportunities, and considerations for both mandatory and voluntary deployments of NG911.
Utilizing Partnerships to Make NG911 Possible	This document lists a variety of resources inside and outside government agencies that should be tapped to ensure proper planning, procurement, and implementation of NG911.
911 Cybersecurity Resource Hub	This webpage contains SAFECOM and the National Council of Statewide Interoperability Coordinators resources for ECCs, including resources for reporting a cyber incident, real world use cases, planning: response and recovery, cybersecurity awareness and training, protecting networks from cyberattacks, design and implementation, and risk assessments.

Data Exchange and Information Sharing Environments

Agencies should perform an evaluation of who the organization most often communicates with, and what types of information are commonly exchanged

Grant recipients using federal funds for data exchange solutions should ensure the solutions comply with OASIS EDXL suite of data messaging standards and NIEM framework

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

Data exchange and information sharing solutions are as fundamental as a digital data "snapshot" transferred over electronic media, or as tailored as custom-interface applications that allow proprietary applications to be linked. Challenges to effective information exchange include increasing types of data being exchanged, such as geographic information systems, evacuee or patient tracking, biometrics, accident and crash telematics, Computer-Aided Dispatch, Automatic Vehicle Location, and more. To communicate seamlessly with the increasingly interconnected systems of the broader community, agencies should consider standards-based information exchange models.

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

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

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

- OASIS EDXL suite of data messaging standards facilitates information sharing among public safety agencies. Grant-funded systems, developmental activities, or services related to emergency response information sharing should comply with the following OASIS and HL-7 standards: "OASIS EDXL-TEP" and Bi-directional Transformation of OASIS EDXL-TEP (Tracking of Emergency Patients) v1.1 and HL7 v2.7.1 Specification Version and OASIS EDXL suite of data messaging standards. Compliance should include the following OASIS EDXL standards:
    - Common Alerting Protocol, version 1.2 or latest version
    - Distribution Element (DE), version 1.0 or latest version
    - Hospital AVailability Exchange (HAVE), version 1.0 or latest version

  - Resource Messaging (RM) standards, version 1.0 or latest version

In efforts to develop an Information Sharing Framework (ISF) to support public safety telecommunications, the SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC) established the Information Sharing Framework Task Force comprised of information technology and communications subject matter experts from public safety agencies across the country. This task force has developed an ISF to ensure effectiveness of new products and technologies as agencies transition to mobile and fully interconnected environments.

To begin using the functional components of the ISF integration layer, public safety agencies should ask the following high-level operational questions:

- What is the content?
- What is the data source?
- Who owns the data?
- Who needs it?
- Over what path?
- Over what application?

A few of the widely used exchange models are provided as part of this appendix; however, an evaluation of who the organization most often communicates with, and what types of information are commonly exchanged, is recommended in selecting an ideal data exchange and information sharing solution. For more information on how to develop and implement an ISF and customize it for various use cases, see the *SAFECOM/NCSWIC Approach for Developing an Interoperable Information Sharing Framework*.

Table B-9. Data Exchange Standards and Resources

Organizations	Standards and Resources
NIEM	Applicants are encouraged to reference the NIEM website to develop a greater understanding of data exchange functions and processes.
GRA	Many Department of Justice grant solicitations require its grant recipients to comply with the GRA, specifically the Global Standards Package, which describes a full information sharing technology standards implementation suite that addresses data standardization, messaging architecture, security, and privacy requirements. For additional information, including technical assistance and training opportunities, visit the Office of Justice Programs website.
OASIS	OASIS Emergency Management Technical Committee creates incident- and emergency-related standards for data interoperability: Common Alerting Protocol; EDXL – Distribution Element; EDXL – Resource Messaging; and EDXL – Tracking of Emergency Clients.
SAFECOM and NCSWIC Information Sharing Framework	SAFECOM and NCSWIC, in coordination with CISA and the Johns Hopkins Applied Physics Laboratory, developed an ISF to help responders to discover, access, and consume any relevant information on a need-to-know basis, regardless of jurisdiction, affiliation, or location.
Information Sharing Assessment Tool	The Information Sharing Assessment Tool, developed by DHS with the guidance of local, state, and federal public safety practitioners, is a tool for public safety officials and first responders to identify their own information sharing capabilities and gaps. It aims to empower communities to develop an action plan to address their most pressing information-sharing gaps; publicize their progress and achievements; and facilitate inter-agency and cross-discipline information sharing.
911 DataPath	This effort is a result of a formal recommendation by the FCC's TFOPA and includes a Strategic Plan and Administrative Dataset for Decision Making.

Appendix C – Emergency Communications Resources

This appendix provides links to references in the *SAFECOM Guidance* and additional resources to help grant applicants develop emergency communications projects and complete DHS grant applications. Visit the SAFECOM website (cisa.gov/safecom) for additional resources.

911 / Next Generation 911 (NG911)

- See Appendix B in the *SAFECOM Guidance*
- National 911 Program Website: 911.gov
    - 911 DataPath: 911.gov/projects/911-datapath/
    - 911 Grant Program: 911.gov/projects/federal-funding
    - *NG911 Standards Identification and Review*: 911.gov/docs-and-tools/#sort=date
    - *NG911 Self-Assessment Tool*: 911.gov/projects/ng911-self-assessment-tool/
    - Webinars: 911.gov/webinars/
    - Federal Funding Programs for 911: 911.gov/projects/federal-funding
- National Association of State 911 Administrators: nasna911.org and nasna911.org/contact-911
- National Emergency Number Association: nena.org

Cybersecurity

- See Appendix B in the *SAFECOM Guidance*
- *NIST Cybersecurity Framework 2.0*: nist.gov/cyberframework
- CISA Cyber Resource Hub: cisa.gov/cyber-resource-hub
- CISA Public Safety Cybersecurity Website: cisa.gov/public-safety-cybersecurity
- Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure

Department of Justice (DOJ)

- *Law Enforcement Tech Guide for Communications Interoperability*: cisa.gov/safecom/planning-resources

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Website: cisa.gov
- Contact Information: ECD@cisa.dhs.gov
- 911 Cybersecurity Resource Hub: SAFECOM/National Council of Statewide Interoperability Coordinators resources for Emergency Communications Centers: cisa.gov/911-cybersecurity-resource-hub
- Identity, Credential, and Access Management Resources and *Trustmark Framework*: cisa.gov/safecom/icam
- *National Emergency Communications Plan*: cisa.gov/national-emergency-communications-plan
- National Interoperability Field Operations Guide: cisa.gov/safecom/field-operations-guides
- Pandemic Guidelines for 911 Centers: cisa.gov/resources-tools/programs/emergency-communications-pandemic-guidance
- Priority Services Programs: cisa.gov/resources-tools/programs/priority-telecommunications-services
- Shared Communication Systems and Infrastructure: cisa.gov/resources-tools/services/shared-communication-systems-and-infrastructure
- Technical Assistance and Training Catalogs: cisa.gov/safecom/ictapscip-resources, dhs.gov/training-technical-assistance, and cisa.gov/resources-tools/resources/cisa-services-catalog
- *Transition to Advanced Encryption Standard*: cisa.gov/sites/default/files/2023-10/23_0918_fpic_AES-Transition-WhitePaper_Final_508C_23_1023.pdf

Federal Communications Commission (FCC)

- FCC Public Safety and Homeland Security Bureau: fcc.gov/public-safety-and-homeland-security
- Contact Information: pshsbinfo@fcc.gov
- FCC Fee Filing Guide for the Wireless Telecommunications Bureau: fcc.gov/licensing-databases/fees/application-processing-fees
- FCC Narrowbanding Website: FCC Narrowbanding
- Communications Security Reliability and Interoperability Council: fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability
- Task Force on Optimal Public Safety Answering Point Architecture: fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point
- FCC 700 MHz Public Safety Broadband Spectrum Guidance: fcc.gov/700-mhz-public-safety-narrowband-spectrum
- FCC 800 MHz Transition: fcc.gov/general/800-mhz-spectrum
- Narrowbanding Guidance
    - *SAFECOM Guidance*, Section 3.3
    - Guidance for licensees for FCC's narrowband operation requirement: https://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html
    - Information on Frequency Coordinators: fcc.gov/general/public-safety-frequency-coordinators
    - Contact Information: narrowbanding@fcc.gov
- *Ending 9-1-1 Fee Diversion Now Strike Force (911 Strike Force) Report*: fcc.gov/911strikeforce
- 911 Fee Reports and Reporting: fcc.gov/general/911-fee-reports

Federal Emergency Management Agency (FEMA)

- FEMA Grants Website: fema.gov/grants
    - Authorized Equipment List: fema.gov/grants/tools/authorized-equipment-list
    - Information Bulletins: fema.gov/grants/preparedness/about/informational-bulletins
    - *Preparedness Grants Manual*: fema.gov/grants/preparedness/manual
- *Comprehensive Preparedness Guide 201*: fema.gov/emergency-managers/national-preparedness/goal/risk-capability-assessment
- Environmental Planning and Historical Preservation (EHP):
    - EHP guidance for DHS/FEMA grant applications: fema.gov/grants/guidance-tools/environmental-historic
    - For questions on EHP for DHS/FEMA grants, contact: GPDEHPInfo@fema.gov
    - For information on federal EHP requirements, see the Council on Environmental Quality Regulations, 40 CFR Part 1500-1508: energy.gov/sites/prod/files/NEPA-40CFR1500_1508.pdf
- Integrated Public Alert and Warning System (IPAWS) Program Office: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system
    - Alerting Authorities and State, Local, Tribal, and Territorial Users: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system
    - Common Alerting Protocol: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/technology-developers/common-alerting-protocol
    - Information Materials: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system
    - IPAWS Best Practices: fema.gov/sites/default/files/documents/fema_ipaws-best-practices-guide.pdf
    - IPAWS Components: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system
    - IPAWS Program Planning Toolkit: fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/toolkit
- Presidential Policy Directive–8: dhs.gov/presidential-policy-directive-8-national-preparedness and fema.gov/emergency-managers/national-preparedness
- National Incident Management System (NIMS): fema.gov/emergency-managers/nims
    - *NIMS Information and Communications Technology (ICT) Functional Guidance*: fema.gov/emergency-managers/nims/components

- NIMS National Standard Curriculum Training Development Guidance: fema.gov/emergency-managers/nims/implementation-training
- National Preparedness Goal: fema.gov/emergency-managers/national-preparedness/goal
- National Preparedness System: fema.gov/emergency-managers/national-preparedness/system
- National Risk Index: fema.gov/flood-maps/products-tools/national-risk-index
- Stakeholder Preparedness Review: fema.gov/emergency-managers/national-preparedness/goal/risk-capability-assessment
- State Administrative Agency Contact List: fema.gov/grants/preparedness/about/state-administrative-agency-contacts
- State Homeland Security Director Office Information: dhs.gov/state-homeland-security-and-emergency-services
- Threat and Hazard Identification and Risk Assessment: fema.gov/emergency-managers/national-preparedness/goal/risk-capability-assessment
- Training: fema.gov/emergency-managers/national-preparedness/training and firstrespondertraining.gov/frts/
  - Homeland Security Exercise and Evaluation Program: fema.gov/emergency-managers/national-preparedness/exercises/hseep
  - Incident Command System Resource Center: training.fema.gov/emiweb/is/icsresource

Federal Grants Information and Listings

- Office of Management and Budget Circulars, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards: https://www.govinfo.gov/app/details/CFR-2025-title2-vol1/CFR-2025-title2-vol1-part200
- Grants.gov Website: grants.gov
- FEMA Grants: fema.gov/grants
- SAFECOM compiled *List of Federal Financial Assistance Programs Funding Emergency Communications*: cisa.gov/safecom/emergency-comms-grants-list

First Responder Network Authority (FirstNet Authority) / Nationwide Public Safety Broadband Network

- FirstNet Authority Website: firstnet.gov
- FirstNet Authority Contact Information: info@firstnet.gov
- NTIA Public Safety Website: https://www.ntia.gov/programs-and-initiatives/public-safety
- Middle Class Tax Relief and Job Creation Act: govinfo.gov/content/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf

SAFECOM / National Council of Statewide Interoperability Coordinators (NCSWIC)

- Best Practices for Planning and Implementation of P25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI): Volume I
- *Contingency Considerations When Facing Reductions in Emergency Communications Budgets*: cisa.gov/sites/default/files/2023-02/22_0302_contingency_planning_fact_sheet_final_508.pdf
- *Contingency Planning Guide for Emergency Communications Funding*: cisa.gov/sites/default/files/2023-02/22_0302_contingency_planning_guide_for_emergency_communcations_funding_final_508.pdf
- Emergency Communications System Lifecycle Planning Guide
- Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials
- *Interoperability Planning for Wireless Broadband*: cisa.gov/sites/default/files/publications/interoperability_planning_wireless_broadband_web_111711.pdf
- *The Funding and the Future of P25 Video*: cisa.gov/resources-tools/resources/p25
- *Funding and Sustaining LMR: Materials for Decisions-Makers*: cisa.gov/safecom/funding
- *Funding Mechanisms Guide for Public Safety Communications*: cisa.gov/sites/default/files/2023-02/21_0621_funding_mechanisms_guide_final_508.pdf
- *NG911 Self-Assessment Tool*: 911.gov/projects/ng911-self-assessment-tool/

- *Operational Best Practices for Encryption Key Management*: cisa.gov/sites/default/files/publications/08-19-2020_Operational-Best-Practices-for-Encryption-Key-Mgmt_508c.pdf
- Project 25 Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) Primer
- Public Safety Communications Dependencies on Non-Agency Infrastructure and Services
- *Public Safety Communications Evolution Brochure*: cisa.gov/sites/default/files/publications/Public_Safety_Communications_Evolution_FINAL_01222019_508C.pdf
- *Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warnings & Notifications*: cisa.gov/sites/default/files/publications/safecom-ncswic_ten_keys_to_improving_awns_4.26.19_-_final_section_508_compliant.pdf
- *Public Safety Communications Resiliency: Ten Keys to Obtaining a Resilient Local Access Network*: cisa.gov/sites/default/files/publications/07202017_10_Keys_to_Public_Safety_Network_Resiliency_010418_FINAL508C.pdf
- Public Safety Communications Network Resiliency Self-Assessment Guidebook
- Regional Interoperability Communications Plan Template
- *SAFECOM Interoperability Continuum*: cisa.gov/sites/default/files/publications/21_0615_cisa_safecom_interoperability_continuum_brochure_final.pdf
- SAFECOM Member List: cisa.gov/safecom/membership
- Statewide Interoperability Coordinator (SWIC): See *SAFECOM Guidance*, Sections 3.2 and 4.2
- Statewide Communication Interoperability Plan (SCIP): See *SAFECOM Guidance*, Sections 2.2 and 4.2
  - CISA SCIP Website: cisa.gov/resources-tools/services/statewide-communication-interoperability-plans-workshops
  - To find your SCIP, please contact your SWIC or SCIP Point of Contact. SWIC contact information can be found on the NCSWIC membership page: cisa.gov/safecom/ncswic-membership

Standards

- SAFECOM Guidance on Technology and Equipment Standards: *SAFECOM Guidance*, Section 4.5 and Appendix B
- Association of Public-Safety Communications Officials standards: apcointl.org/services/standards/
  - Project 43: Broadband Implications for the PSAP: apcointl.org/technology/next-generation-9-1-1/project-43-broadband-implications-for-the-psap/
- Data Exchange and Information Sharing Environment: See Appendix B in the *SAFECOM Guidance*
  - National Information Exchange Model: niem.gov
  - OASIS, Standards for Data-Related Investments: oasis-open.org
  - Information Sharing Assessment Tool: dhs.gov/science-and-technology/isat
- Long-term evolution (LTE) for Public Safety Broadband: See Appendix B in the *SAFECOM Guidance*
  - 3GPP RAN5 Mobile Terminal Conformance Testing: 3gpp.org/3gpp-groups/radio-access-networks-ran/ran-wg5
- NENA i3 Solution – Stage 3: nena.org/page/standards
- NIST List of Certified Devices: nist.gov/ctl/pscr/process-document-nist-list-certified-devices
- Project 25 (P25) Standards for Land Mobile Radio: standards.tiaonline.org/standards/technology/project_25/index.cfm
  - P25 Technology Interest Group: project25.org
  - P25 Compliance Assessment Program: dhs.gov/science-and-technology/p25-cap
  - P25 Compliance Assessment Program list of approved radio equipment: dhs.gov/science-and-technology/approved-grant-eligible-equipment
  - Statement of P25 User Needs (SPUN): cisa.gov/resources-tools/resources/p25-resources

Technology

- SAFECOM Guidance on Technology and Equipment Standards: *SAFECOM Guidance*, Section 4.5 and Appendix B

- Unmanned Aircraft Systems (UAS)
    - *Cybersecurity Guidance Chinese-Manufactured UAS*
    - *Department of Defense Blue UAS Policy and Cleared List*
    - *Public Safety Uncrewed Aircraft System Resource Guide*
    - *Responding to Drone Calls: Guidance for Emergency Communications Centers*

Appendix D – Compliance Requirements for DHS Grants

This appendix provides assistance 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 requirements for DHS/FEMA grants. For additional information, see relevant sections within the *SAFECOM Guidance*. Below is a non-exhaustive description of DHS/FEMA recipients should also refer to the specific Notice of Funding Opportunity or the *Preparedness Grants Manual* for all programmatic requirements that apply (fema.gov/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	Your grant application must: • Describe how your proposed projects will support the national goals and objectives in the National Emergency Communications Plan (NECP). • Describe how your 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. Contact information for SWICs can be found on the NCSWIC membership page. • Explain how your proposed projects will address or support communications resiliency.
Project Coordination Sections 2.1, 2.2, 2.4, 3.2, 3.3	• List all participants who are involved in project planning to show that there is engagement with the whole community in accordance with Presidential Policy Directive-8 and the NECP. • Develop projects that are regional, multi-jurisdictional, multi-disciplinary, and cross-border to promote greater interoperability across agencies. This will help you to 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. The SWIC will help establish statewide plans, policies, and procedures, and coordinate decisions on communications investments that are 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	NIMS Implementation Objectives: • You must identify the specific NIMS implementation criteria that will be used to be eligible for FEMA preparedness grants. In addition, some grants may have additional NIMS training or personnel credentialing criteria (see the applicable Notice of Funding Opportunity for details). • States, territories, and tribal grant recipients will need to report on NIMS implementation annually in the Stakeholder Preparedness Review (SPR). States, territories, and tribal grant recipients must submit their annual SPR through the Unified Reporting Tool (URT). They must also email a copy of the URT submission to their respective DHS/FEMA Regional Federal Preparedness Coordinator, and cc FEMA at fema-spr@fema.dhs.gov. SPR submissions are due no later than December 31 each year.
Spectrum Licensing Section 3.3	• If a project requires a new spectrum license, consult the appropriate statewide coordinator (e.g., SWIC), the Federal Communications Commission, and/or the FirstNet Authority to ensure the recipient will have the authority to operate in the desired spectrum. Spectrum consultation should begin prior to submitting your application or during the early phases of an approved project. A spectrum license must be in place before any associated equipment can be purchased.

Topics	Requirements
Planning and Organization Sections 2.2, 3.4, 4.2	• As a grant recipient, you must update and submit the SPR and Threat and Hazard Identification and Risk Assessment (THIRA). The Comprehensive Preparedness Guide 201 provides a three-step process for conducting a THIRA/SPR. Follow THIRA/SPR submission instructions in program guidance. • Complete and submit the Nationwide Cybersecurity Review, if required by program guidance, to benchmark and measure progress towards improving cybersecurity posture.
Training Sections 2.3, 4.3	• In your grant application, describe how proposed training projects will support the NIMS Training Program, how they are consistent with NECP priorities, and how they will address gaps identified through your state or territory's SCIP, After-Action Reports, and other assessments.
Exercises Section 2.3, 4.4	• When conducting exercises, include participants from multiple jurisdictions, disciplines, and different levels of government, and private sector entities, when appropriate. See FEMA exercise guidance for more information. • Manage and execute exercises in accordance with the Homeland Security Exercise and Evaluation Program.
Equipment Section 4.5	• As a grant recipient, you must ensure equipment that any procurements comply with the covered telecommunications restrictions outlined in the John S. McCain National Defense Authorization Act of 2019 as outlined in FEMA Policy #405-143-1.
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. 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. • You must 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 preparedness grants, and the P25 Compliance Assessment Program Approved Equipment List. If you intend for your grant proposal to include any non-P25 LMR equipment, you will need to 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 to emergency responders. If your 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 at 911.gov.
Public Safety Broadband Sections 2.5, 4.5, 5, Appendix B	• Consult with applicable governing bodies and leaders for the latest guidance from the FirstNet Authority on planning for public safety broadband network activities, and identifying the authority to operate on public safety spectrum. For additional information, refer to firstnet.gov.
Alerts, Warnings, and Notifications 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 to alert, warn, and notify the public with public safety information simultaneously via 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 your proposal includes alerts and warnings, review IPAWS informational materials and Common Alerting Protocol standard.