Emergency Communications Preparedness Center: Federal Financial Assistance Reference Guide

Recommendations and Resources for Federal Program Managers of Emergency Communications Funding

2016

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

The Emergency Communications Preparedness Center (ECPC) is an interagency coordinating body that supports and promotes the ability of emergency responders and government officials to communicate in the event of natural or man-made disasters and to enhance interoperable emergency communications nationwide.[1] The ECPC Executive Committee recognized the need to better coordinate federal programs that support emergency communications, and requested the ECPC Grants Focus Group (GFG) to develop common guidance for these programs.

In response to this request, the ECPC GFG developed the *ECPC Recommendations to Federal Agencies: Financial Assistance for Emergency Communications* (*ECPC Grants Recommendations Document*). Since its first release in 2010, the *ECPC Grants Recommendations Document* has provided a strategy for federal financial assistance programs that fund emergency communications—including grants, loans, and cooperative agreements. The *ECPC Grants Recommendations Document*, updated in 2013, identified three priorities the ECPC GFG and member agencies will focus over the subsequent three to five years and outlines recommended actions that support the following ECPC GFG priorities:

1) Promote consistency in policy across federal financial assistance programs that fund emergency communications;
2) Coordinate across federal agencies and financial assistance programs to support the advancement of emergency communications; and
3) Improve the understanding of emergency communications funding.

The ECPC GFG priorities are essential in the work of federal program managers overseeing emergency communications financial assistance programs, particularly when providing guidance to grantees and stakeholders who wish to apply or interested in applying for emergency communications funding. To assist federal program managers in understanding these priorities and implementing recommended actions, the ECPC GFG developed this *ECPC Federal Financial Assistance Reference Guide* (*ECPC Reference Guide*) in conjunction with the *ECPC Grants Recommendations Document* in 2013.[2] Since then, the ECPC GFG updated the *ECPC Reference Guide* in 2016 to reflect developments in the emergency communications ecosystem, changes affecting the grants community, and provide resources for federal program managers.

To request access to ECPC GFG documents, federal program managers can register on the ECPC Clearinghouse, which resides on the MAX website (https://max.omb.gov) and allows members to share emergency communications information. Additional information about the ECPC GFG is located in this guide's attachment.

[1] The ECPC was authorized in Section 652 (c) of the Post-Katrina Emergency Management Reform Act of 2006 (P.L. 109-295). For more information on the ECPC, see: http://www.dhs.gov/emergency-communications-preparedness-center.
[2] In previous years, technical standards and resources were included within the *ECPC Grants Recommendations Document.* In 2013, the ECPC GFG separated the content into a long-term strategy to improve federal coordination and this *ECPC Reference Guide* containing critical information affecting emergency communications programs.

1.2 PURPOSE

The *ECPC Reference Guide* provides common guidance for federal program managers to use when developing notices of funding opportunities (NOFO), award agreements, performance and financial reports, and other program materials. This guide includes:

- Overview of the grants landscape, national plans, and programs affecting emergency communications;
- Common grant guidelines for applicants of emergency communications funds; and
- Resources and tools for federal program managers to understand policies and technical standards that promote interoperability among federally-funded investments.

By using this guide, federal program managers support the ECPC GFG efforts to improve emergency communications investments through greater coordination and consistency in federal financial assistance programs.

1.3 HOW TO USE THIS DOCUMENT

The ECPC GFG designed the *ECPC Reference Guide* to assist federal program managers in the process of developing or updating individual program materials. Table 1 provides step-by-step instructions for federal program managers using this guide.

Table 1. Instructions for Using this Guide

Steps for Federal Program Managers to Take Before Developing Materials	Refer to Appropriate Section	To Complete this Step, Federal Program Managers Should…
Step 1: Understand the issues, national plans, and programs that impact emergency communications projects	Section 2: Understanding the Emergency Communications Grants Landscape	Action 1: Incorporate key initiatives and national plans with individual program goals during planning stages
Step 2: Review *SAFECOM Guidance* to understand stakeholder-driven priorities for emergency communications funding	Section 3.1: SAFECOM Guidance on Emergency Communications Grants	Action 2: Insert language referencing the *SAFECOM Guidance* into program materials to encourage applicants to use it during project development
Step 3: Identify applicable policies and technical standards based on the type of projects individual program will fund, in addition to those referenced in *SAFECOM Guidance*	Section 3.2: Project-Specific Recommendations	Action 3: Insert applicable project-specific recommendations into NOFOs and grant agreements
Step 4: Understand the ECPC GFG data collection effort to identify projects and supporting financial data	Section 3.3: Data Collection to Understand Emergency Communications Funding Nationwide	Action 4: Insert recommended language in NOFOs for applicants to self-identify emergency communications projects and track financial data
Step 5: Review resources and tools to use during Pre-Award, Award, Post Award, and Closeout phases	Section 4: Supporting Materials to Use throughout the Grant Cycle	Action 5: Direct applicants to applicable resources and available federal funding that may assist all phases of their project development

While these steps help guide federal program managers to support individual programs funding emergency communications, the ECPC GFG is also available to answer questions, discuss issues, and assist with identifying applicable requirements upon request. The ECPC GFG will review the *ECPC Reference Guide* periodically and modify as information on emergency communications plans and initiatives, policies, and technical standards evolve. Send any questions or comments on this document to the ECPC GFG at ECPC@hq.dhs.gov.

2. UNDERSTANDING THE EMERGENCY COMMUNICATIONS GRANTS LANDSCAPE

This section describes the emergency communications ecosystem, national plans, and federal programs that fund emergency communications. In order to promote consistent policies and coordination across programs, federal program managers should understand these aspects of the emergency communications grants landscape before developing individual program materials. This document provides federal program managers with information to determine which changes to the landscape are applicable to individual financial assistance programs.

2.1 EMERGENCY COMMUNICATIONS ECOSYSTEM

A more complex and interdependent emergency communications ecosystem has emerged, due to evolving technologies, risks, and stakeholders, impacting many facets of emergency communications. Federal program managers should review these topics and incorporate relevant initiatives and information into individual program materials.

2.1.1 Developments in Advanced Technologies

Traditionally, land mobile radio (LMR) networks are the primary systems that the public safety community use for mission-critical voice communications. To augment their LMR capabilities, public safety agencies are increasingly using commercial wireless broadband services and, in some cases, procuring private broadband networks for mission-critical data communications. Internet Protocol (IP)-enabled networks have the potential to transform how public officials will communicate by providing connectivity and bandwidth that enhance situational awareness and information sharing.

Once deployed, the Nationwide Public Safety Broadband Network (NPSBN) will provide the public safety community with wireless broadband data communications to augment their mission-critical voice communications. The initial focus is not to replace the current mission-critical voice transmission networks, but to complement it by enabling the transmission of digital data in a variety of formats. The NPSBN will be deployed on a single nationwide, standards-based architecture, making it critical for federal investments to align with and support the final network architecture selected by the First Responders Network Authority (FirstNet) and for the FirstNet architecture to align with previously existing network architectures.[3] Further, state-level networks must also align with FirstNet requirements to ensure interoperability and compatibility. Full deployment of the NPSBN will take years, requiring state and local jurisdictions to sustain current mission-critical communications capabilities and follow FirstNet guidance.

[3] FirstNet is responsible for the building, deployment, and operation of a nationwide interoperable public safety broadband network with a single national architecture to ensure interoperability for public safety entities. FirstNet is the single licensee for the combined public safety broadband spectrum band (763-768 MHz and 793-798 MHz) and D Block spectrum (758-763 MHz and 788-793 MHz).

Communication network modernization is also occurring with the migration of the Nation's 911 infrastructure to Next Generation 911 (NG911), an IP-based model that will enable the transmission of both voice and data (e.g., texts, images, video) from the public to 911 Public Safety Answering Points (PSAPs), between PSAPs, and eventually on to emergency responders. Also, the deployment of a nationwide public alerting system is using IP-based technologies to transmit alerts to mobile phones and other devices. To sustain LMR systems while deploying new broadband technologies, legacy 911 systems and alerting systems will continue to serve the public's needs until new systems are in place.

2.1.2 Risks

Emergency communications systems will be able to transmit sensitive data, such as law enforcement information and electronic medical records, which create new security considerations including the secure transmission, storage, and access, to the information. While electronic access to this data enables more effective response operations, it also exposes the system to new risks including system failures, lack of user or server connection, and hostile hackers. As the community adopts new technologies and applications, it must increase understanding and planning for the security risks associated with the open architecture and vast complexity of IP-based technologies and services.

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

The convergence of technologies and risks in the evolving ecosystem reinforces the importance of ongoing planning for emergency communications. Federal program managers should convey these considerations to their grantees, so that all components of all existing, broadband, cyber, and IP-based technologies are included in strategic plans and common operational protocols.

2.1.3 Stakeholders

In addition to technological developments and associated risks, the Nation's approach to preparing for and responding to emergency events and incidents is also evolving. The *Presidential Policy Directive (PPD) 8: National Preparedness* establishes the National Preparedness Goal, a national approach to preparedness that promotes a shared responsibility across all levels of government, private and nonprofit sectors, including businesses, non-governmental organizations, and the general public.[4] By providing the necessary knowledge and skills, the Federal Government seeks to enable the whole community to contribute to and benefit from national preparedness.[5] Financial assistance programs must contribute to the National

[4] For more information on PPD-8, see: http://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[5] For more information on the whole community, see: http://www.fema.gov/national-preparedness/whole-community.

Preparedness Goal and strengthen national preparedness by planning for their most relevant and urgent risks.

2.2 NATIONAL PLANS

By understanding key initiatives, federal program managers are able to develop individual programs that align with the policies and plans across the Federal Government. The ECPC GFG serves as an information resource to federal program managers ensuring new policies and changes in the emergency communications grants landscape are widely known and supported as they are released. This is important as financial assistance programs serve as one of the primary mechanisms to implement federal policy and make progress on key initiatives in partnership with state, local, tribal, and territorial governments.

Federal program managers should review national plans and ensure that individual programs support national emergency communications policies. Aligning with federal financial assistance programs will ensure that recipients' projects support and advance their respective goals and objectives to improve emergency communications, and support consistency across the Nation. The ECPC GFG has identified four national plans that focus on different aspects of emergency communications, provided in Table 2.

Table 2. Summary of National Plans

National Plan	Description	Emergency Communications Funding Guidance/Elements
National Emergency Communications Plan (NECP)[6]	The NECP establishes a national strategy focused on ensuring the Nation's emergency response community can communicate and share information across levels of government, jurisdictions, disciplines, and organizations for all hazards, as needed and when authorized. It aims to maximize the use of all communications capabilities available to emergency responders—voice, video, and data—and to ensure the security of data and information exchange.	The NECP emphasizes the need to enhance and update the policies, governance structures, plans, and protocols that enable responders to communicate and share information under all circumstances. Federal program managers should encourage applicants to coordinate with state-level personnel and communications plans to ensure that federally-funded projects align to statewide plans, are coordinated, and are not duplicative.

[6] Title XVIII of the Homeland Security Act of 2002 (6 United States Code 101 et seq.), as amended, requires the Department of Homeland Security (DHS) to develop the NECP. For more information, see: http://www.dhs.gov/necp.

National Plan	Description	Emergency Communications Funding Guidance/Elements
National Preparedness Goal (NPG) and National Preparedness System (NPS)[7]	The NPG and NPS were established to strengthen security and systematic preparation of the Nation towards its greatest threats. The NPG is: *"A secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."* The NPS outlines an organized process for the whole community to move forward with preparedness activities to achieve the NPG.	Federal program managers should encourage applicants to coordinate with state-level personnel to ensure that emergency communications needs are included in risk assessments, such as the Threat and Hazard Identification Risk Assessment (THIRA).[8] Coordination with state-level personnel supports the whole community approach outlined in the NPS and the President's plan to improve overall preparedness.
National Infrastructure Protection Plan (NIPP)[9]	The NIPP establishes national priorities and requirements for critical infrastructure protection to build a safer, more secure, and more resilient Nation by preventing, deterring, neutralizing, or mitigating the effects of all hazards and to strengthen national preparedness, timely response, and rapid recovery.	Federal program managers should require applicants to show how proposed emergency communications projects (e.g., assets, networks, systems) are secure, resilient, and can be rapidly restored after a natural or man-made disaster. Requiring applicants to build resilience into projects during their establishment will help to secure our Nation's critical infrastructures.
Next Generation 911 (NG911) Migration Plan[10]	The NG911 Migration Plan establishes a plan for migrating to a national Internet Protocol (IP)-enabled emergency network capable of receiving and responding to all citizen-activated emergency communications and improving information sharing among all emergency response entities.	Federal program managers should encourage applicants to consult State-level personnel when proposing projects to enhance 911 services to ensure they support statewide plans and the NG911 Migration Plan. The Middle Class Tax Relief and Jobs Creation Act of 2012 provides the National Highway Traffic Safety Administration (NHTSA) with $115 million for grants to improve 911 services. Grantees should continue to monitor current Federal actions affecting broadband and 911 programs funded through the Act.[11]

Figure 1 demonstrates how federal program managers can align their programs to national plans when developing individual program materials. Above all, the ECPC GFG recognizes that federal program managers must follow federal-wide requirements and agency-specific mission and policies that guide their financial assistance programs. Federal program managers have some flexibility in defining program goals, eligible costs, and activities with consideration of the authorizing legislation and the program's unique purpose and priorities. The ECPC GFG recommends that federal program managers review national plans and identify relevant goals and

[7] PPD-8 requires DHS to develop the NPG and NPS. For more information, see: http://www.fema.gov/national-preparedness-goal and http://www.fema.gov/national-preparedness-system.
[8] For more information on THIRA, see: http://www.fema.gov/media-library/assets/documents/26338?fromSearch=fromsearch&id=5825.
[9] PPD-7 requires DHS to develop the NIPP, available at: https://www.dhs.gov/national-infrastructure-protection-plan.
[10] The New and Emerging Technologies 911 Improvement Act of 2008 tasked the Department of Transportation's National 911 Office with developing the NG911 Migration Plan. For more information, see: http://www.911.gov/standardsfornextgen.html. .
[11] Updates on the 911 Grant Program will be posted on the National 911 Program's website when funding becomes available. For more information, see: http://www.911.gov/.

objectives that their individual program can support, while also supporting the aforementioned requirements and priorities.

Figure 1. Approach for Aligning Individual Programs to National Plans

When reviewing national plans and determining applicability to individual programs, federal program managers may consult with the respective lead agencies of national plans and the ECPC GFG to understand the impact to emergency communications.

2.3 FEDERAL PROGRAMS FUNDING EMERGENCY COMMUNICATIONS

Several federal financial assistance programs are available to state, local, tribal, and territorial governments and other entities that want to invest in emergency communications. The ECPC GFG coordinates across these federal programs, which are summarized in Table 3. Federal programs may become available or cease funding depending on annual appropriations laws. For more information on each program, refer to Section 4, Table 8, or visit the SAFECOM website (www.dhs.gov/safecom) to learn about the current fiscal year's federal funding opportunities.

Table 3. Summary of Federal Programs Funding Emergency Communications

Department	Agency / Office	Program Name
Department of Agriculture (USDA)	Rural Utilities Services (RUS)	• Community Connect Programs • Community Facilities Programs • Telecommunications Infrastructure Loans
Department of Commerce (DOC)	National Telecommunications and Information Administration (NTIA)	• State and Local Implementation Grant Program (SLIGP) • *Future FirstNet implementation program**
Department of Homeland Security (DHS)	Federal Emergency Management Agency (FEMA)	• Assistance to Firefighters Grant (AFG) • AFG Fire Prevention and Safety (FP&S) • Emergency Management Performance Grant (EMPG) • Homeland Security Grant Program (HSGP) o State Homeland Security Program (SHSP) o Urban Areas Security Initiative (UASI) o Operation Stonegarden (OPSG) • Tribal Homeland Security Grant Program (THSGP) • Non-Profit Security Grant Program (NSGP) • Port Security Grant Program (PSGP) • Transit Security Grant Program (TSGP) • Intercity Bus Security Grant Program (IBSGP)

Department	Agency / Office	Program Name
	Science and Technology (S&T) Directorate	• Small Business Innovation Research (SBIR)
Department of Health and Human Services (HHS)	Assistant Secretary for Preparedness and Response (ASPR)	• Hospital Preparedness Program (HPP)
	Center for Disease Control and Prevention (CDC)	• Public Health Emergency Preparedness (PHEP)
Department of Justice (DOJ)	Community Oriented Policing Services (COPS)	• Coordinated Tribal Assistance Solicitation (CTAS) • Community Policing Development (CPD)
	Office of Justice Programs (OJP)	• Edward Byrne Memorial Justice Assistance Grant Program (JAG)
	National Institute of Justice (NIJ)	• Research Grants in Law Enforcement, Geospatial, and Criminal Justice Information Technology
Department of Transportation (DOT)	National 911 Program	• *911 Grant Program**

** Denotes anticipated federal programs that will fund emergency communications.*

3. COMMON GRANT GUIDELINES FOR EMERGENCY COMMUNICATIONS

While it is essential for federal program managers to understand issues affecting the emergency communications grants landscape, it is equally important for applicants to understand these issues. This section provides common grant guidelines for applicants to understand priorities, best practices, and technical standards when developing emergency communications projects. Federal program managers can reference or insert these common grant guidelines into individual program materials as resources for applicants.

3.1 SAFECOM GUIDANCE ON EMERGENCY COMMUNICATIONS GRANTS

The *SAFECOM Guidance on Emergency Communications Grants* (*SAFECOM Guidance*) is developed for entities applying for federal financial assistance for emergency communications projects.[12] The *SAFECOM Guidance* provides general information on eligible activities, technical standards, and other terms and conditions that are common to most federal emergency communications programs. Specifically, the *SAFECOM Guidance* provides guidance to applicants on:

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

The ECPC GFG recommends that federal agencies reference the *SAFECOM Guidance* in applicable program materials, and encourage applicants to use it when planning and investing in emergency communications projects. By referencing the *SAFECOM Guidance* in individual program materials, federal agencies can provide recipients with the policies, resources, and expectations surrounding emergency communications projects from the onset and help to ensure federally-funded projects are coordinated, compatible, and interoperable. The ECPC GFG considers this reference fundamental, as it enables federal program managers to include all recommendations for emergency communications projects, no matter the project type. Federal agencies may also choose to select applicable policies, technical standards, and best practices to include in individual program materials, as described in Section 3.2, Table 4.

[12] DHS works with the ECPC GFG, SAFECOM members, and the National Council of Statewide Interoperability Coordinators to develop the *SAFECOM Guidance* annually. For more information, see: http://www.dhs.gov/safecom.

3.2 PROJECT-SPECIFIC RECOMMENDATIONS

This section provides federal program managers with project-specific recommendations to consider and include in individual program materials. The ECPC GFG developed these project-specific recommendations based on the input and best practices prescribed by its member agencies. These project-specific recommendations mirror the information included in the *SAFECOM Guidance* for applicants. While referencing the *SAFECOM Guidance* includes the content in this section, federal agencies may also emphasize certain policies, technical standards, or guidelines to applicants by inserting project-specific recommendations for emergency communications projects. For project-specific recommended language that federal program managers can copy/paste into individual program materials, see Section 4, Table 5.

Table 4 summarizes the best practices that federal program managers can include as project-specific recommendations in their individual programs. This step is an optional addition to referencing the *SAFECOM Guidance*, as described in Section 3.1. By incorporating these project-specific recommendations, federal program managers will help applicants prioritize federal funding in alignment with national plans.

Table 4. Summary of Project-Specific Recommendations

Topic	Description
Best Practice: Coordination with Emergency Communications Leaders Encourage/Require applicants to consult statewide emergency communications leaders prior to application submission. This ensures that projects are coordinated and consistent with statewide plans. There are several leadership and governance structures that have been established over time, including:	
Statewide Interoperability Executive Committee (SIEC) / Statewide Interoperability Governing Board (SIGB)	A SIEC or SIGB is a statewide governing body that includes representatives from various jurisdictions, disciplines, as well as subject matter experts. • To find the SIGB or SIEC for the state, contact your SWIC or OEC at oec@hq.dhs.gov
Statewide Interoperability Coordinator (SWIC)	The SWIC serves as a central coordinator for the state or territory on emergency communications issues and oversees the daily operation of the state's interoperability efforts, including updating and implementing the Statewide Communication Interoperability Plan. • http://www.dhs.gov/statewide-interoperability-coordinators
FirstNet State Single Point of Contact	Each Governor designated a single officer or governmental body to serve as coordinator with FirstNet and planning for the NPSBN, as well as implementation of the State and Local Implementation Grant Program funds. • http://www.ntia.doc.gov/category/state-and-local-implementation-grant-program
Senior Advisory Committee (SAC)	The SAC is a governance group composed of multiple stakeholders responsible for creating a cohesive planning framework that builds and implements preparedness initiatives. • https://www.fema.gov/media-library/assets/documents/103698
911 Advisory Board / 911 Administrator	The 911 Administrator manages the state or territory's 911 functions as determined by state legislation. The 911 Advisory Board works with the 911 Administrator to plan and coordinate State and local 911 efforts. • http://www.nasna911.org/state-911-contacts • https://resourcecenter.911.gov/code/9-1-1ProfileDatabase.aspx

Topic	Description
Best Practice: Alignment of Projects to Emergency Communications Plans Encourage/Require applicants to align projects to existing emergency communications plans. Aligning projects to plans helps to ensure that federally-funded projects support—and do not contradict—statewide emergency communications efforts. There are several emergency communications plans available, including:	
Statewide Communication Interoperability Plan (SCIP)	SCIPs are locally-driven, multi-jurisdictional statewide plans that define the current and future vision for communications interoperability within the state or territory. • http://www.dhs.gov/statewide-communication-interoperability-plans
State-level Broadband Plan	A comprehensive plan, as part of existing SCIP or similar plans that describes the public safety needs expected to be addressed in its design of the NPSBN. • http://www.ntia.doc.gov/other-publication/2013/sligp-federal-funding-opportunity
State 911 Deployment Plan	Many states have developed 911 deployment plans for enhanced wireless and NG911 capabilities. • http://www.nasna911.org/state-911-contacts
Regional Interoperable Communications Plan (RICP)	RICPs document regional strategies for achieving communications operability and interoperability. • http://www.dhs.gov/emergency-communications-guidance-documents-and-publications
Tactical Interoperable Communications Plan (TICP)	TICPs document the interoperable communications resources available in a designated state, region, or urban area. • http://www.dhs.gov/emergency-communications-guidance-documents-and-publications
Best Practice: Demonstration of How Projects Address Critical Needs Defined in Assessments Encourage/Require applicants to conduct assessments, or reference existing assessments, to demonstrate how the proposed project addresses mission-critical needs. This ensures that the project is necessary and supported by the state. Emergency communications assessments include:	
Capability Assessments	Capability assessments document the capabilities, resources, and assets available for emergency response situations. For example, the NECP outlines three strategic goals, which were used to evaluate selected area's ability to demonstrate response-level communications during planned events in 2010 and county-level response in 2011. As a result, each participating area has an NECP Goal Assessment that provides information on response capabilities and needs. • http://www.dhs.gov/national-emergency-communications-plan-necp-goals
Risk Assessments	Risk assessments allow jurisdictions to effectively identify risks—including risks to emergency communications systems and procedures—and allocate resources to address gaps and achieve capability targets.
State 911 Assessment Program	The goal of the statewide 911 assessment program is to provide peer feedback on the operational capabilities of a statewide 911 system based on a set of objective benchmarks. • http://www.911.gov/state911assessment.html
After-Action Reports (AAR) and Improvement Plans	An AAR summarizes exercise events, evaluates performance, and analyzes if goals and objectives of the exercise were met. Improvement plans convert lessons learned from the exercise into concrete, measurable steps to improve response by detailing actions to address each AAR recommendation and the timeline for completion.
Best Practice: Investment in Training Training improves emergency response by helping ensure personnel are proficient in procedures and the use of equipment. Training must be continuously given as new personnel join emergency responder agencies and updated to reflect the evolution of communications technologies. Support localities' training investments and encourage/require applicants to enroll in federally-sponsored training programs for emergency communications personnel, including:	
National Incident Management System (NIMS)	NIMS establishes standardized incident management processes, protocols, and procedures that all emergency responders use to coordinate and conduct response actions. • http://www.fema.gov/national-incident-management-system

Topic	Description
NIMS Incident Command System (ICS) Communications Unit Program	ICS is a standardized, on-scene, all-hazards incident management approach that provides emergency responders with a method and processes to lead a coordinated response. There is training for ICS-certified positions including All-Hazards Communications Unit Leader (COML) and All-Hazards Communications Technician (COMT). • https://www.fema.gov/incident-command-system-resources
Emergency Support Function (ESF) Annex #2 – Communications	ESF Annex #2 provides the approach that the Federal Government uses to support emergency responders when their communication systems have been impacted by large-scale incidents. • http://www.fema.gov/media-library/assets/documents/32174?id=7351
Best Practice: Investment in Exercises Exercises are a key component of national preparedness as they provide stakeholders with the opportunity to plan, practice, and assess performance during a planned incident and identify areas for improvement. Encourage/Require applicants to include an exercise element in proposed projects to demonstrate and test the capability purchased with federal funds, and then report on the investment's effectiveness. The Federal Government has developed guidelines for exercises, including:	
Homeland Security Exercise and Evaluation Program (HSEEP)	HSEEP provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design, conduct, evaluation, and improvement planning. HSEEP supports national efforts to leverage the whole community to build, sustain, and deliver core capabilities that will improve response. • http://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf
Best Practice: Adherence to Technical Standards that Promote Interoperability Encourage/Require recipients to invest in standards-based equipment so that federally-funded projects are compatible and interoperable with surrounding systems. As technologies continue to evolve faster than standards development, federal program managers must work with recipients to adhere to existing standards and plan to incorporate future standards. The ECPC GFG identified recommendations based on the emergency communications capability: LMR, IP-enabled, data information sharing, broadband, 911, and public alerting systems.	
Land Mobile Radio (LMR) Standards	
Project 25 (P25)	P25 provides a suite of standards that define technical specifications to allow equipment to interoperate, regardless of manufacturer. The P25 Compliance Assessment Program (CAP) is a voluntary program allowing P25 equipment suppliers to formally demonstrate their products' compliance with a select group of requirements by testing it in recognized laboratories. • http://www.tiaonline.org/standards/tia-standards-overview
Voice Over Internet Protocol (VoIP) Standards	
Voice-over-Internet Protocol (VoIP) Standards	VoIP allows for the transmission of real-time voice services through IP-based networks. Bridging Systems Interface (BSI) and Project 25 Inter Radio Frequency Sub-System Interface (ISSI) are two interfaces between two bridging or gateway devices. • http://www.pscr.gov/downloads/press/voip-npstc_newsletter_032009.pdf
Data-Related Information Sharing Standards	
National Information Exchange Model (NIEM)	NIEM is a framework for exchanging information that provides common terminology for users and a repeatable, reusable process for developing information exchange requirements. NIEM allows disparate systems to share, exchange, accept, and translate information in an efficient manner that all users can understand. • https://www.niem.gov
OASIS Emergency Data eXchange Language (EDXL)	OASIS EDXL is a suite of data messaging standards provided in the following areas: common alerting protocol; distribution element; hospital availability exchange; resources messaging; reference information model; situation reporting; and tracking emergency patients. • https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=emergency
Information Sharing Environment (ISE) Initiative	The ISE is the people, projects, systems, and agencies that enable responsible information sharing across the national security enterprise. The ISE initiative provides standards, guides, and best practices for technology implementation and data information sharing processes. • https://www.ise.gov/

Topic	Description
Emerging Technology and Broadband Standards	
Wireless Fidelity (Wi-Fi)	Wi-Fi networks use radio technologies to connect electronic devices to one another or access points connected to the Internet. Wi-Fi networks operate in the unlicensed 2.4 and 5 gigahertz (GHz) radio bands, with some products supporting both bands (i.e., dual-band). • http://www.wi-fi.org/
Long-Term Evolution (LTE)	LTE is a wireless broadband worldwide 3GPP standard that enables high-speed data transmission (e.g., pictures, streaming video, mobile incident command, and complex mapping applications) via a cellular architecture. The NPSBN will use LTE. • http://www.firstnet.gov/content/lte-technology
Next Generation 911 (NG911) Standards	
NG911 Standards	NG911 will seamlessly connect public safety answering points (PSAP) and will allow for the transmission and reception of multimedia type data (e.g., text messages, pictures, and video). These standards are currently under development. As NG911 standards continue to evolve, stakeholders should consult the *NG911 Standards Identification and Review* to ensure that solutions developed or procured meet industry guidelines and standards. • http://www.911.gov/standardsfornextgen.html
Public Alerts and Warning System Standards	
Integrated Public Alert and Warning System (IPAWS) Profile and Common Alerting Protocol (CAP)	IPAWS provides emergency responders with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, the IPAWS All-Hazards Information Feed, and other public alerting systems from a single interface. IPAWS uses the CAP international data standards. • http://www.fema.gov/integrated-public-alert-warning-system • https://www.fema.gov/common-alerting-protocol
Best Practice: Consultation of Federal Resources when Purchasing Equipment There are several federal resources that provide assistance to applicants planning to purchase emergency communications equipment. Encourage applicants to reference the following federal resources:	
SAFECOM Website	The SAFECOM website provides resources for emergency communications stakeholders, including the *SAFECOM Guidance,* guidelines for developing a Statement of Requirements (SoR), and a list of financial assistance programs that fund emergency communications. • http://www.dhs.gov/safecom
Standardized Equipment List (SEL)	The SEL is a voluntary guidelines equipment list, created by the InterAgency Board, including descriptions of communications equipment, important features, operating considerations, training requirements, and applicable users. • https://iab.gov/SELint.aspx
Public Safety Communications Research (PSCR) Program	The PSCR Program provides research, development, testing, and evaluation for voice, data, image, and video communications. The PSCR Program offers resources for applicants researching communications equipment options. • http://www.pscr.gov/projects/projects_about.php

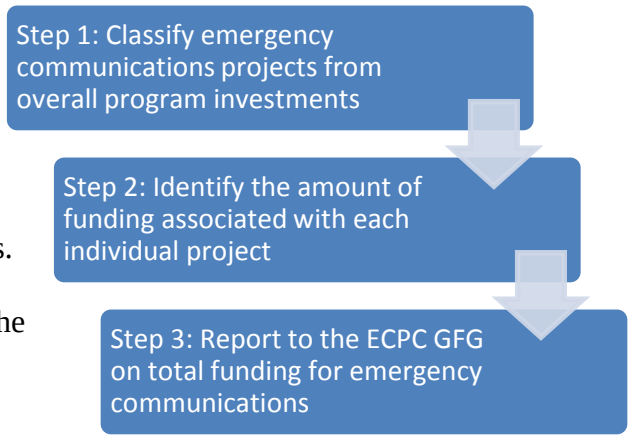
Topic	Description
Public Safety Tools	*Communications Asset Survey and Mapping (CASM) Tool*: A standardized collection method for emergency responders to store and display data about their communications assets and how the assets are used. *Emergency Communications System Life Cycle Planning Guide*: A step-by-step process for designing, implementing, supporting, and maintaining an emergency communications system. *National Interoperability Field Operations Guide (NIFOG)*: A reference guide for radio technicians and communications planners. *State/Local and Tribal Response Level Communications Tools*: A reporting capability to independently assess response-level emergency communications involving multiple agencies. • http://www.publicsafetytools.info/start_index_v2.php
Best Practice: Consultation with Spectrum Authorities The Federal Communications Commission (FCC) and FirstNet authorize public safety entities to use specific spectrum bands to operate emergency communications systems. There have been several changes to the public safety spectrum band, such as the narrowbanding mandate, 800 MHz reconfiguration, and changes to the 700 MHz broadband spectrum band. Federal program managers should consult spectrum authorities as needed and provide guidance to applicants on the following spectrum issues:	
Ultra-High Frequency (UHF) / Very High Frequency (VHF) Narrowbanding	The FCC mandated that all non-federal LMR licensees operating between 150 and 512 MHz and using 25 kilohertz (kHz) bandwidth voice channels migrate to 12.5 kHz bandwidth or equivalent efficiency by January 1, 2013. While the deadline has passed, many public safety entities are still working toward compliance. • http://transition.fcc.gov/pshs/public-safety-spectrum/narrowbanding.html
700 MHz Narrowbanding	The FCC has eliminated the requirement for further narrowbanding of 700 MHz public safety narrowband systems from 12.5 kHz down to 6.25 kHz bandwidth. • http://www.npstc.org/TBand.jsphttp://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1024/FCC-14-172A1.pdf
800 MHz Reconfiguration	Directed by the FCC, parts of the 800 MHz private radio band shared by public safety and industry must be reconfigured to eliminate interference. The 800 MHz reconfiguration is ongoing and will separate spectrum used by public safety systems and commercial cellular wireless networks within the 800 MHz band. An independent 800 MHz Transition Administrator oversees the reconfiguration process, establishes reconfiguration guidelines, and provides resources for entities affected by the rebanding. • http://www.800ta.org/
T-Band Migration	The Middle Class Tax Relief and Job Creation Act of 2012 authorized the future auction of the 470–512 MHz ultra-high frequency band, referred to as the T-Band. The Act requires those licensees to migrate from the T-Band to other, unspecified spectrum, within nine years (i.e., by 2021), and requires T-Band public safety licensees to relocate from the T-Band to other, unspecified spectrum, two years after the completion of the auction of this spectrum.
700 MHz Public Safety Broadband Spectrum	The Middle Class Tax Relief and Job Creation Act of 2012 authorized the establishment of the NPSBN and dedicated broadband spectrum for its users. The Act designated the combined 700 MHz public safety band and D Block for NPSBN use and named FirstNet as the single licensee for the combined spectrum. Incumbents currently operating in this band may need to migrate from the band to clear the spectrum for NPSBN use as early as 2017. FirstNet has announced that it will establish a grant program to support such relocation by qualified licensees. • http://www.npstc.org/TBand.jsp

Topic	Description
Best Practice: Ensuring Communications System Security Communications between emergency responders should be secure. Support investments in procurements and activities that will improve the security of communications systems.	
Project 25 - Advanced Encryption Standard (AES)	AES is a cryptographic algorithm that allows for secure communications among devices that are enabled with AES encryption capability. The Federal Government recognizes the 256-bit AES as a robust encryption algorithm and strongly recommends entities migrate to AES. • http://www.npstc.org/download.jsp?tableId=37&column=217&id=3287&file=DHS_Guidelines_for_Encryption_in_LMR_Systems.pdf
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	ICS-CERT offers resources and training that may be helpful to emergency communications personnel, as well as best practices and a repository of cyber control system standards and expertise that system operators can use to improve security on emergency communications systems. • http://ics-cert.us-cert.gov/
Best Practice: Participation in Priority Telecommunications Services Emergency responders have access to priority telecommunications services and priority service restoration provided through the Federal Government. These services can greatly improve the ability of emergency response providers at all levels of government to communicate in emergencies. Support participation and any user fees associated with the priority telecommunications services.	
Priority Telecommunications Services	Emergency responders have access to priority telecommunications services and priority service restoration provided through the Federal Government. These priority services include the Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS), Telecommunications Service Priority (TSP), and eventually IP-based priority services. • http://www.dhs.gov/oec-communications-portfolio-management

3.3 DATA COLLECTION TO UNDERSTAND EMERGENCY COMMUNICATIONS FUNDING NATIONWIDE

The ECPC GFG prioritizes data collection on emergency communications funding to assist programs in assessing programmatic and national impact to emergency communications nationwide. As the Federal Government looks to improve the accessibility and use of data, federal agencies are under pressure to demonstrate the impact and effectiveness of financial assistance programs. The development of new reporting requirements provides federal agencies the opportunity to incorporate emergency communications data collection elements as agencies review and modify data collection systems. For example, the Digital Accountability and Transparency Act of 2014, P.L. 113-101, requires the Department of the Treasury and the Office of Management and Budget to transform U.S. federal spending from disconnected documents into open, standardized data, and to publish that data online.[13] Eventually, all federal agencies will be required to report standardized data and make that information available to the public. The ECPC GFG works with its members to identify improvements for data collection on emergency communications funding within the changing landscape of federal data requirements.

Figure 2. ECPC GFG Data Collection Steps



[13] For more information on the DATA Act, see: https://www.gpo.gov/fdsys/pkg/PLAW-113publ101/pdf/PLAW-113publ101.pdf.

Specifically, federal program managers can categorize emergency communications related-projects, which in turn helps to identify the total amount of emergency communications-specific funding within programs and across agencies. The next step toward gaining a better understanding of emergency communications funding is to identify the amount of funding associated with each individual project. In the last step, federal program managers should extract financial data on emergency communications projects and report to the ECPC GFG on total funding for emergency communications.

The action steps outlined above are general guidance on data gathering. The ECPC GFG has developed several emergency communications-specific data collection elements to help federal program managers analyze and report on the effectiveness of funding, as well as to assess the level and impact of their respective federal financial assistance programs for emergency communications. For more information and the ECPC GFG data collection template, see Section 4, Table 14.

4. SUPPORTING MATERIALS TO USE THROUGHOUT THE GRANT CYCLE

Materials are organized by the grant life cycle to support programmatic activities during each phase—Pre-Award, Award, Post Award, and Closeout. However, federal program managers may use these materials at any time during the development and administration of emergency communications programs. Federal program managers may also contact the ECPC GFG (ECPC@hq.dhs.gov) for questions or comments on the following materials:

Pre-Award
- Recommended Language for Individual Program Materials
- Glossary of Emergency Communications Terms

Award
- Financial and Programmatic Issues when Reviewing Applications
- List of FY 2015 Federal Programs that Fund Emergency Communications

Post Award
- Project 25 Activities and Key Words
- Next Generation 911 Activities and Key Words
- Broadband Activities and Key Words
- Status of Public Safety Broadband Projects

Closeout
- ECPC GFG Data Collection Template

4.1 PRE-AWARD

This section provides resources for federal program managers when announcing funding opportunities, supporting applicants in the process of completing grant applications, and reviewing applications. Below includes recommended language to insert into grant program materials, as well as a glossary of emergency communications terms to use during the Pre-Award phase.

4.1.1 Recommended Language for Individual Program Materials

Table 5 includes recommended language for federal program managers to use when developing program materials, including notices to announce their individual programs. The language is sorted by common emergency communications-related topics. Federal program managers may contact the ECPC GFG to develop language on topics not included.

Table 5. Recommended Language for Federal Grant Program Materials

Topic	Recommended Language
Reference to *SAFECOM Guidance*	Recipients (including sub-recipients) that are using federal funds for emergency communications activities should comply with the *SAFECOM Guidance for Emergency Communication Grants (SAFECOM Guidance)*, including provisions on technical standards that ensure and enhance interoperable communications. The *SAFECOM Guidance* is available at: http://www.dhs.gov/safecom.
Coordination with Emergency Communications Leaders	Prior to application submission, applicants interested in investing federal funds in emergency communications projects should coordinate with statewide emergency communications leaders (e.g., Statewide Interoperability Governing Body, Statewide Interoperability Coordinator, FirstNet state-level point of contact, State 911 Administrator) to ensure the project supports the statewide strategy to improve emergency communications, is compatible and interoperable with surrounding systems, and is not duplicative.
Alignment of Projects to Emergency Communications Plans	Applicants interested in using federal funds for emergency communications should ensure that proposed projects support statewide strategies and plans (e.g., Statewide Communication Interoperability Plan, Regional Interoperable Communications Plan) to improve emergency communications. Applicants should coordinate with statewide emergency communications leaders (e.g., Statewide Interoperability Governing Body, Statewide Interoperability Coordinator) to obtain strategies and relevant plans. Applicants should describe how activities support statewide strategies and align to relevant emergency communications plans.
Demonstration of How Projects Address Critical Needs	Applicants interested in using federal funds for emergency communications are strongly encouraged to reference existing emergency communications assessments (e.g., National Emergency Communications Plan Goal Assessments, risk assessments, after-action reports) to ensure the proposed projects meet the assessments' mission-critical needs. Applicants should provide a brief narrative of the need as defined in the assessment, and describe how the proposed project will help to address that need.
Investment in Training	Federal funds may be used to support emergency communications-specific training, including training on communications protocols, plans, and equipment, as well as nationally-recognized communication training programs (e.g., National Incident Management System/Incident Command System, All Hazards Communications Unit Leader, All Hazards Communications Technician, and Emergency Support Function #2)
Investment in Exercises	Applicants interested in using federal funds for emergency communications are strongly encouraged to include an exercise at project completion to demonstrate the new capabilities gained and gauge the investment's effectiveness. Applicants should use the Homeland Security Exercise and Evaluation Program, which provides a national standard and best practices for exercise design, development, conduct, evaluation, and improvement planning. For more information, see: https://hseep.dhs.gov.
LMR P25 Standards	Applicants proposing to purchase digital voice land mobile radio (LMR) systems and equipment with federal funds should ensure equipment is compliant with Project 25 (P25), unless otherwise noted in the program guidance. Applicants are strongly encouraged to obtain documented evidence from the manufacturer that the equipment has been tested and passed all the applicable, published, and normative P25 compliance assessment test procedures for performance, conformance, and interoperability, as defined by the P25 Compliance Assessment Program (CAP). If documentation is not available through the P25 CAP, applicants should obtain documented evidence from the manufacturer that the equipment has been tested and passed all of the applicable, published, and normative P25 test procedures for performance, conformance, and interoperability. Applicants requesting federal funds to replace or add radio equipment to an existing non-P25 system, such as procuring new portable radios for an existing analog system, should provide a compelling reason for non-standard equipment to be purchased. Applicants must provide written justification of how the non-standard equipment will advance interoperability and how the purchase will support eventual migration to interoperable systems. Otherwise, applicants considering new radio or system acquisitions are expected to invest in standards-based equipment and migrate to P25-compliant equipment. When federal funds are used to purchase new P25 LMR systems and equipment containing non-standard features or capabilities, and a comparable P25 feature or capability is available, applicants must ensure the standards-based feature or capability is included as well. Further, if federal funds are used to upgrade existing systems and equipment or to add non-standard features or capabilities, and a comparable P25 feature or capability is available, applicants must ensure that the standards-based feature or capability is included as well.

Topic	Recommended Language
VoIP Standards	When purchasing bridging or gateway devices that have a Voice over Internet Protocol (VoIP) capability to provide connectivity between land mobile radio (LMR) systems, devices purchased with federal funds must, at a minimum, implement either the Bridging Systems Interface (BSI) specification or the P25 Inter Radio Frequency Sub-System Interface (ISSI) as a part of their VoIP capability. Applicants should see standards posted at: http://www.pscr.gov/outreach/archive/safecom_archive/voip/BSIIntroduction123009_v2.pdf
Data-Related Information Sharing Standards	Applicants proposing projects that support emergency response information sharing should leverage the National Information Exchange Model (NIEM) during project development to understand and incorporate data component or element standards into the project. NIEM has developed specific guidance for applicants, which can be found at: https://www.niem.gov/aboutniem/grant-funding/Pages/implementation-guide.aspx. Further, all federally-funded investments involving data exchange technologies should comply with the Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data eXchange Language (EDXL) suite of data messaging standards and NIEM guidelines. Additional information on data messaging standards and their applicability may be found at: http://www.oasis-open.org.
Acquisition and Deployment of Broadband Technologies	Applicants investing in broadband technologies should be aware that the Federal Government is developing a Nationwide Public Safety Broadband Network (NPSBN). The development of technical standards for the network is underway, and statewide planning to identify users and assess needs is in progress. Applicants are encouraged to engage in planning for the NPSBN at the state-level. Applicants proposing the acquisition and deployment of broadband projects that will operate in the 700 megahertz (MHz) public safety broadband spectrum (758–769 MHz and 788–799 MHz) should be aware that granting agency will review broadband-related proposals closely. Applicants should demonstrate in applications that the project: • Has authority from FirstNet to operate in the public safety broadband spectrum; • Has been coordinated with statewide broadband planners; • Supports the statewide plan for broadband; • Complies with FirstNet technical requirements (when issued); and • Will integrate into the NPSBN.
NG911 Standards	Applicants are encouraged to consult the Next Generation 911 (NG911) Migration Plan, standards review documents, and assessment guidelines when planning projects to enhance public safety answering points (PSAP) or emergency communications systems that interface with PSAPs. Applicants seeking federal funds for NG911 projects should comply with the requirements of the National 911 Program Office or applicable funding source agency, including provisions on technical standards that ensure interoperable communications. Unless otherwise stated, equipment must meet all mandatory standards to be eligible for purchase using these funds. In addition, applicants should obtain all necessary certifications and licenses for the requested equipment. Information on NG911 standards is available at: http://www.911.gov/standardsfornextgen.html.
Investment in Public Alerting	Applicants interested in using federal funds for public alert and warning systems are encouraged to consult the Integrated Public Alert and Warning System (IPAWS) Program Management Office (PMO) or website (http://www.fema.gov/integrated-public-alert-warning-system) prior to planning to understand how the project can use IPAWS resources to enhance alerting. In order to access IPAWS, applicants must select equipment that adheres to both Common Alerting Protocol (CAP) and IPAWS Profile standards. Contact the IPAWS PMO at ipaws@fema.gov.
Consultation with Federal Resources when Purchasing Equipment	Applicants seeking federal funds for emergency communications equipment should ensure that equipment complies with technical standards for interoperability. Applicants should leverage resources such as the SAFECOM website (http://www.dhs.gov/safecom), the Standardized Equipment List (https://iab.gov/SELint.aspx), and the Public Safety Communications Research Program (http://www.pscr.gov/index.php) before purchasing equipment to understand technical requirements and ensure equipment is tested and compliant with applicable technical standards that promote interoperability. In addition, there are several public safety tools that may assist with project planning (e.g.,Communications Asset Survey and Mapping Tool) available at: http://www.publicsafetytools.info/start_index.php.

Topic	Recommended Language
UHF / VHF Narrowbanding	Applicants are encouraged to allocate federal funds (where allowable) to implement narrowbanding activities that will ensure compliance with Federal Communications Commission (FCC) narrowband mandate that all non-federal land mobile radio (LMR) licensees operating between 150 and 512 MHz and using 25 kHz bandwidth voice channels migrate to 12.5 kHz bandwidth or equivalent efficiency by January 1, 2013. Recipients should prioritize funding toward: replacing non-narrowband compliant equipment; acquiring/upgrading additional tower sites to maintain coverage after conversion; and reprogramming existing equipment to operate in compliance with the narrowband mandate. Recipients should also ensure that existing LMR systems are compliant with narrowbanding requirements and consult with statewide emergency communications leaders (e.g., Statewide Interoperability Coordinator) and the FCC on any non-compliance issues to avoid admonishment, monetary fines, or loss of license.
Projects in the 800 MHz Band	Applicants contemplating communication projects in areas still undergoing 800 MHz rebanding should consult statewide emergency communications leaders (e.g., Statewide Interoperability Coordinator), the Federal Communications Commission, and the 800 MHz Transition Administrator, which is responsible for overseeing the rebanding process and providing technical assistance to affected licensees.
T-Band Migration	Applicants seeking funding for relocation of T-Band systems should consult the Federal Communications Commission, statewide emergency communications leaders (e.g., Statewide Interoperability Coordinator), and a frequency coordinator early in the project development process to ensure the project supports statewide plans for improving emergency communications, and is planned in the appropriate spectrum.
Securing LMR Communications	Applicants planning to use federal funds to purchase encryption options for new or existing communications equipment should ensure that encrypted capabilities are compliant with the Project 25 (P25) Block Encryption Protocol. Applicants investing in encryption technology are strongly encouraged to invest in Advanced Encryption Standards (AES) 256-bit. The P25 suite of standards references the use of AES and Data Encryption Standard-Output Feedback (DES-OFB) in the Project 25 Block Encryption Protocol, ANSI/TIA-102.AAAD. Applicants seeking to use federal funds to purchase non-standard encryption features or capabilities for new or existing equipment must ensure AES is included, as well as ensure their devices have the capability to interoperate in an encrypted mode. Applicants currently using DES-OFB may continue to invest in this encryption method but should plan to migrate to AES as soon as possible. The Federal Government recognizes AES as a more robust encryption algorithm and strongly recommends entities migrate to AES to ensure future interoperability with federal entities.
Securing Advanced IP-Based Technologies	Applicants investing in advanced Internet-Protocol (IP) –based technologies should consult statewide emergency communications leaders (e.g., Statewide Interoperability Coordinator, Statewide Interoperability Governing Body) to ensure systems comply with statewide security standards. Applicants should also consult relevant federal program offices (e.g., Industrial Control System Cyber Emergency Response Team) and reference federal resources to understand risks and ensure the security of systems.
Participation in Priority Telecommunications Services	Federal funds may be used to facilitate participation in priority telecommunications services if the organization is a state, local, tribal, or territorial police department, fire department, public safety answering point or 911 call center, emergency medical service, essential health care provider, or any other organization that requires communication services to protect the public health and safety and maintain law and order. Applicants should leverage programs designed for priority service and call completion, such as the Government Emergency Telecommunications Service (GETS), the Telecommunications Service Priority (TSP), and the Wireless Priority Service (WPS).
Identify Emergency Communications Projects	• Yes/No Question: Does this project include expenditures or investments for emergency communications? • Project Narrative Requirement: Provide a narrative that describes the proposed emergency communication expenditures. • Equipment List Requirement: If applicable, provide a list of emergency communications equipment purchased through the financial assistance program.

4.1.2 Glossary of Emergency Communications Terms

Federal program managers are encouraged to reference the glossary in Table 6 when developing program materials and supporting applicants in completing their applications. The glossary of emergency communications terms is from the *2014 National Emergency Communications Plan*.

Table 6. NECP Glossary of Emergency Communications Terms

Term	Definition
After-Action Report (AAR)	A professional document formulated in partnership with participants in a process. Evaluators, sponsoring agencies, and key participants from government agencies participate in the formulation of the after-action report. It furnishes a historical record of findings and forms the foundation for refinements to plans, policies, procedures, training, equipment, and overall preparedness of an entity. The report depicts the process, preliminary observations, and major issues, and makes recommendations for improvements.
Applications	A set of features and a user interface that may be realized by fixed or mobile devices. User services are logical building blocks of application-layer functionality.
Agreements	Formal mechanisms to govern interagency coordination and the use of interoperable emergency communications solutions.
Assessment	The process of acquiring, collecting, processing, examining, analyzing, evaluating, monitoring, and interpreting the data, information, evidence, objects, measurements, images, and sound, among others, whether tangible or intangible, to provide a basis for decision-making.
Amateur Radio Service	A radio communication service for the purpose of self-training, intercommunication, and technical investigations carried out by amateurs, who are duly authorized persons interested in radio technique solely with a personal aim and without pecuniary interest.
Auxiliary Communications	Backup emergency radio communications provided by volunteers who support public safety and emergency response professionals and their agencies.
Broadband	High-speed Internet that allows users to access the Internet and Internet-related services at significantly higher speeds than those available through dial-up Internet access services. Broadband allows users to access information via the Internet using one of several high-speed transmission technologies: Digital Subscriber Line; Cable Modem; Fiber; Wireless; and Satellite. Transmission is digital, meaning that text, images, and sound are all transmitted as bits of data. The transmission technologies that make broadband possible move these bits much more quickly than traditional telephone or wireless connections.
Common Alerting Protocol	The Common Alerting Protocol is a digital format for exchanging emergency alerts that allows a consistent alert message to be disseminated simultaneously over many different communications systems.
Communications Unit	Within the Incident Command System, an organizational unit in the Logistics Section that is responsible for effective incident communications planning, especially in the context of a multi-agency incident. Additionally, this unit installs and tests all communications equipment, supervises and operates the incident communications center, distributes and recovers communications equipment assigned to incident personnel, and maintains and repairs communications equipment on site.
Continuity of Communications	The ability of emergency response agencies to maintain communications capabilities when primary infrastructure is damaged or destroyed.
Core Capabilities	Distinct critical elements necessary to achieve the *National Preparedness Goal*.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: *2013 National Infrastructure Protection Plan*)
Cross-Discipline	Involving emergency response providers from different disciplines (e.g., police, fire, emergency medical services).
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information

Term	Definition
	networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: *2013 National Infrastructure Protection Plan*)
Dispatch Center	Agency or interagency dispatch centers, 911 call centers (e.g., public safety answering points), emergency control or command dispatch centers, or any naming convention given to the facility and staff that handles emergency calls from the public and communication with emergency management/response personnel.
Emergency Communications	The means and methods for exchanging communications and information necessary for successful incident management.
Emergency Management Assistance Compact	A congressionally ratified mutual aid compact that legally establishes a national system to facilitate resources across State lines during an emergency or disaster.
Emergency Response Providers	The Homeland Security Act of 2002 defines emergency response providers as federal, state, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.
Emergency Support Functions (ESF)	Used by the Federal Government and many state governments as the primary mechanism at the operational level to organize and provide assistance. ESFs align categories of resources and provide strategic objectives for their use. ESFs utilize standardized resource management concepts such as typing, inventorying, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.
Exercises	Instruments to train for, assess, practice, and improve performance in prevention, protection, mitigation, response, and recovery capabilities in a risk-free environment. Exercises can be used for testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; improving individual performance; identifying gaps in resources; and identifying opportunities for improvement.
First Responder Network Authority (FirstNet)	An independent authority within the National Telecommunications and Information Administration that will plan, construct, and operate the first high-speed, nationwide network dedicated to public safety.
First Responders	See "emergency response provider." (The Implementing the 9/11 Commission Recommendations Act of 2007 states that the term first responder shall have the same meaning as the term emergency response provider, which is defined in the Homeland Security Act of 2002.)
Government Emergency Telecommunications Service (GETS)	Service that provides national security and emergency preparedness (NS/EP) personnel priority access and prioritized processing in the local and long distance segments of the Public Switched Telephone Network (PSTN), greatly increasing the probability of call completion. GETS is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a normal call is reduced.
Governance	Relates to consistent management, cohesive policies, guidance, processes, and decision-rights for a given area of responsibility.
Incident Action Plan (IAP)	An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods.
Incident Command System (ICS)	A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small and large, complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations.
Information Sharing Environment	Broadly refers to the people, projects, systems, and agencies that enable responsible information sharing for national security.
Internet Protocol (IP)-Based Technologies	Any component, device, application, or system designed to function on an IP network.
Interoperability	Ability of emergency responders to communicate among jurisdictions, disciplines, frequency bands, and levels of government as needed and as authorized. System operability is required for system interoperability.

Term	Definition
Jurisdiction	A range or sphere of authority. Public safety agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., federal, state, tribal, local boundary lines) or functional (e.g., law enforcement, public health).
Land Mobile Radio Systems	Terrestrially-based wireless narrowband communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works companies, and even the military to support voice and low-speed data communications.
Lifecycle Planning	The process of designing, implementing, supporting, and maintaining a land mobile radio or mobile data-based public safety communications system. Enables practitioners to better forecast long-term funding requirements and helps to set the framework for establishing and maintaining a public safety system.
Long-Term Evolution	The next evolution of commercial broadband wireless communications technology, which was developed to address the demand for high-speed, data intensive communications, such as situational awareness, advanced analytics, database queries, and video applications.
Mission Areas	Groups of core capabilities, including Prevention, Protection, Mitigation, Response, and Recovery. (Source: *National Preparedness Goal*)
Multi-jurisdictional	Involving agencies from different jurisdictions (e.g., across State, county, or regional boundaries).
Mutual Aid Agreement or Assistance Agreement	Written or oral agreement between and among agencies, organizations, or jurisdictions that provides a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, or after an incident.
National Emergency Communications Plan (NECP)	The Homeland Security Act of 2002, as amended, requires DHS to develop the *National Emergency Communications Plan*; the Plan serves as the Nation's only strategic plan for improving emergency response communications and efforts in the United States.
National Incident Management System (NIMS)	Provides a systematic, proactive approach and template to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment.
National Preparedness Goal	The cornerstone for the implementation of Presidential Policy Directive-8, it establishes the capabilities and outcomes for the Nation to accomplish across five mission areas (Prevention, Protection, Mitigation, Response, and Recovery) in order to be secure and resilient. The Goal establishes distinct core capabilities and corresponding target elements for each mission area.
Nationwide Public Safety Broadband Network (NPSBN)	A dedicated, wireless, interoperable, communications long-term evolution-based network that allows public safety to receive and share critical information with their counterparts across the Nation.
National Response Framework (NRF)	A guide to how the Nation responds to all types of disasters and emergencies. It describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters.
National Security and Emergency Preparedness (NS/EP) Communications Functions	The ability of the Federal Government to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions. This includes the survivable, resilient, enduring, and effective communications, both domestic and international, that are essential to enable the executive branch to communicate within itself and with: the legislative and judicial branches; state, local, tribal, and territorial governments; private sector entities; and the public, allies, and other nations.
Nongovernmental Organization (NGO)	As noted in the NRF, these include voluntary, racial and ethnic, faith-based, veteran-based, and nonprofit organizations that provide sheltering, emergency food supplies, and other essential support services. NGOs are inherently independent and committed to specific interests and values.
Operability	Ability of emergency responders to establish and sustain communications in support of mission operations.
Operating Environment	For the purposes of the NECP, this refers to the people, processes, policies, and technologies for emergency communications.
Private Sector Entity	Per the NRF, private sector entities include large, medium, and small businesses; commerce, private cultural and educational institutions; and industry, as well as public-private partnerships that have been established specifically for emergency management purposes.

Term	Definition
Public Safety Entity	An entity that provides public safety services and that include services provided by emergency response providers, as defined in the Homeland Security Act of 2002 (see above definition for "emergency response providers"). (Source: Middle Class Tax Relief and Job Creation Act of 2012)
Public Safety Services	Includes services defined in the Communications Act of 1934 as those with the sole or principal purpose of which is to protect the safety of life, health, or property; that are provided—by state or local government entities; or by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and that are not made commercially available to the public by the provider. Also includes services provided by emergency response providers, as defined in Section 2 of the Homeland Security Act of 2002 (see above definition for "emergency response providers").
Public Safety Answering Point (PSAP)	A facility that has been designated to receive 911 calls and route them to emergency services personnel. A PSAP may act as a dispatch center. PSAP is often used with the term Public Safety Communications Center. (Source: Communications Act of 1934, as amended)
Reliability	Achieved in public safety land mobile radio systems through equipment redundancy and minimizing single points of failures through careful system design. System operators stock spare parts and, in some cases, transportable backup systems to restore system failures that do occur. Reliability must be considered at the earliest stages of system design.
Redundancy	Additional or alternate systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.
Resources	Personnel and major items of equipment, supplies, and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an Emergency Operations Center.
Response-Level Emergency Communications	Per the 2008 NECP, response-level emergency communications are the capacity of individuals with primary operational leadership responsibility to manage resources and make timely decisions during a multi-agency incident without technical or procedural communications impediments. In addition to communicating to first-level subordinates in the field, the Operations Section Chief should be able to communicate upwards to the incident command level (e.g., between the Operations Section Chief and Incident Command).
Social Media	Refers to the means of interactions among people in which they create, share, or exchange information and ideas in virtual communities and networks.
Standard Operating Procedures (SOP)	Generally refers to a reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.
Strategic Planning	Planning process that establishes organizational goals and identifies, scopes, and establishes requirements for the provisioning of capabilities and resources to achieve them.
Statewide Communication Interoperability Plan (SCIP)	Stakeholder-driven, multi-jurisdictional, and multi-disciplinary statewide plans that outline and define the current and future vision for communications interoperability within the state or territory. The SCIP is a critical strategic planning tool to help states prioritize resources, establish and strengthen governance, identify future technology investments, and address interoperability gaps.
Statewide Interoperability Coordinator (SWIC)	Serves as the state's single point of contact for interoperable communications and implements the SCIP.
Statewide Interoperability Governing Bodies (SIGB)	Serves as the primary steering group for the statewide interoperability strategy. Its mission is to support the SWIC in efforts to improve emergency response communications across the state through enhanced data and voice communications interoperability. They often include representatives from various jurisdictions, disciplines, as well as subject matter experts.
Statewide Interoperability Executive Committees (SIEC)	Used interchangeably with Statewide Interoperability Governing Bodies.
Tactical Interoperable Communications Plan (TICP)	A plan providing rapid provision of on-scene, incident based mission critical voice communications among all first responder agencies (e.g., emergency medical services, fire, and law enforcement), as appropriate for the incident, and in support of an incident command system as defined in NIMS.

Term	Definition
Technical Assistance	Support to state, local, tribal, and territorial emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities.
Technology	Per the *SAFECOM Interoperability Continuum*, applies to a capability element that encompasses the systems and equipment that enable emergency responders to share information efficiently and securely during an emergency incident, and addresses the functionality, performance, interoperability, and continuity capabilities of those systems and equipment.
Telecommunications Service Priority (TSP)	A program that authorizes NS/EP organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. The TSP program provides service vendors a FCC mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.
Usage	Per the *SAFECOM Interoperability Continuum*, this applies to the frequency and familiarity with which emergency responders use interoperable emergency communications solutions.
Wireless Priority Service (WPS)	Service offering that provides NS/EP personnel with priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing the probability of call completion. It is intended to be used in an emergency or crisis situation when cellular networks are congested and the probability of completing a normal cellular call is reduced.
Whole Community	Per the *National Preparedness Goal*, the term whole community applies to the 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, local, tribal, and territorial governmental partners in order to foster better coordination and working relationships.

4.2 AWARD

This section provides federal program managers with resources to use during the Award phase. Resources include a list of financial and programmatic issues, challenges, and suggested actions for federal program managers when reviewing applications. Additionally, a list of federal programs that federal program managers could suggest to stakeholders seeking additional funding opportunities for emergency communications activities.

4.2.1 Financial and Programmatic Issues When Reviewing Applications

The Nation's ability to improve mission-critical emergency communications capabilities hinges on successful collaboration between federal program managers and stakeholders. As federal program managers coordinate with applicants and recipients during the grant life cycle, they are faced with several issues that may impact emergency communications projects. By addressing these common financial and programmatic issues in individual program materials, federal program managers can help applicants comply with federal requirements from the onset, potentially saving time and resources throughout the grant life cycle. Table 7 provides a list of financial and programmatic challenges that federal program managers may face when administering emergency communications funding programs, as well as suggested remediation actions.

Table 7. Financial and Programmatic Issues, Challenges, and Suggested Actions

Issue	Challenge	Suggested Federal Program Manager Actions
Funding and sustaining personnel	Federal grant funding levels fluctuate and often restrict personnel costs, making it difficult for entities to sustain personnel for emergency communications efforts	• Ensure program materials detail constraints on personnel costs • Request applicants to describe how they will sustain emergency communications personnel beyond the period of performance without federal funding • Discuss sustainment strategies as part of the monitoring process
Funding and sustaining capabilities	Reductions in federal funding and new focus on broadband is challenging recipient's ability to sustain current capabilities (e.g., LMR systems)	• Encourage recipients to: o Coordinate resources to sustain current capabilities while also planning for the NPSBN o Coordinate with federal granting agency and state-level planners before developing broadband projects to ensure projects support state plans o Plan projects before purchasing equipment
Investing in regional, multi-discipline, and cross-border capabilities	The Federal Government requires recipients to build emergency communications capabilities that serve multiple agencies, jurisdictions, and disciplines; and across borders	• Encourage recipients to coordinate with state-level planners to ensure projects align to state-level plans and assessments, and that projects are compatible with existing systems • Encourage recipients to leverage regional bodies to coordinate resources and projects that will: o Enable communications across jurisdictions, disciplines, and among all levels of government o Expand coverage to unserved or underserved areas o Link disparate systems
Ensuring funds are used for intended purposes	Recipients are required to use funds for purposes stated in the application, but desire flexibility to direct funding toward critical mission areas as needed	• Ensure program materials detail program constraints on eligible activities and costs • Establish clear requirements and processes for award change requests • Encourage stakeholders to work with other granting agencies and eligible applicants to use all available financial assistance programs and resources for emergency communications
Cost sharing and matching funds	Recipients must adhere to different federal agency match requirements	• Ensure program materials detail federal, agency, and program match requirements (e.g., program funds cannot be matched with other federal funds) • Establish clear requirements and processes for match waivers
Commingling or duplication of funds	Since multiple agencies are involved in communications projects, projects are often funded with multiple grants, creating a risk of commingling and duplication	• Ask recipients (and sub-recipients) to detail what portions or phases of their project (e.g., specific sites, equipment, activities) are funded under the award or other awards • Ensure program materials detail requirements on maintaining records that identify the source and application of funds provided for financially-assisted activities
Supplanting	Local communications budgets are decreasing; recipients may seek to use federal grant funds to replace personnel	• Be explicit in program materials that recipients may not: o Use state or local funds that have already been funded or budgeted for the same purpose o Defray any costs that they are already obligated to pay
Compliance with federal procurement requirements	Recipients must ensure that procurements are fair and competitive	• Require recipients to comply with federal procurement policies in *SAFECOM Guidance* • Encourage recipients to include technical standards requirements in response for proposals prior to vendor selection • Monitor recipients to ensure procurements promote open and free competition

Issue	Challenge	Suggested Federal Program Manager Actions
Compliance with federal environmental and historic preservation (EHP) requirements	EHP reviews are required for construction (e.g., towers, shelters) and may affect periods of performance	• Detail EHP requirements and approval processes in NOFOs and other program materials • Require recipients to include milestones for completing zoning/permitting needed for EHP approvals

4.2.2. List of FY 2015 Federal Programs that Fund Emergency Communications

Table 8 summarizes federal financial assistance opportunities that support emergency communications. The ECPC GFG updates this list with fiscal year funding amounts each year and publishes it at http://www.dhs.gov/safecom/funding. Please note that other federal financial assistance opportunities may exist. The ECPC GFG recommends that any entity seeking emergency communications-related funding refer to http://www.grants.gov to determine if other opportunities are available. In addition, entities should refer to the specific notice of funding opportunity, as this is a summary of program information, eligibility, and allowable costs related to emergency communications and does not reflect all program requirements.

Table 8. FY 2015 Federal Programs that Fund Emergency Communications

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
Department of Agriculture (USDA)			
USDA Rural Utilities Service (RUS)	Community Connect The Community Connect program serves rural communities where broadband service is least likely to be available, but where it can make a tremendous difference in the quality of life for citizens. Projects funded by these grants will help rural residents tap into the enormous potential of the Internet. http://www.rd.usda.gov/programs-services/community-connect-grants	Eligible Applicants: State and local governments, federally-recognized Tribes, nonprofits, for-profit corporations Formula-based: Matching funds of at least 15%	Equipment: Construction, expansion, improvement or acquisition of community center; broadband expansion, construction of communication towers
USDA RUS	Community Facilities Community Facilities programs provide loans, grants, and loan guarantees for essential community facilities in rural areas. Priority is given to health care, education, and public safety projects. http://www.rd.usda.gov/programs-services/community-facilities-direct-loan-grant-program	Eligible Applicants: Municipalities, counties, parishes, boroughs, special-purpose districts, non-profit corporations or associations, and Tribal governments Competitive: Applicants will be carefully scored and prioritized to determine which projects should be selected for further development and funding	Planning and Organization: Costs of acquiring interest on land Equipment: Construction and development of hospitals, health clinics, schools, fire houses, community centers, and many other community-based initiatives
USDA RUS	Telecommunications Infrastructure Loan - Expansion of 911 Through the Expansion of 911 Loan, USDA will leverage public and private resources to speed the rural deployment of dual-use public safety/commercial wireless networks, address homeland security communications needs along America's rural international borders, and finance enhanced 911 capabilities for carriers and communities. http://www.rd.usda.gov/programs-services/telecommunications-infrastructure-loans-loan-guarantees	Eligible Applicants: Public bodies, community based non-profit corporations, and federally-recognized Tribes Competitive: Eligible grant projects are selected based on specific criteria in the NOFO	Planning and Organization: Acquisitions and refinancing Equipment: Improvement, expansions, and construction of 911 activities and services related to emergency response efforts

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
Department of Homeland Security (DHS)			
DHS Federal Emergency Management Agency (FEMA)	Assistance to Firefighters Grant (AFG) The primary goal of the AFG program is to meet the firefighting and emergency response needs of fire departments and non-affiliated emergency medical service organizations. The AFG provides support for resources needed to protect the public and emergency personnel from fire and related hazards. http://www.fema.gov/assistance-firefighters-grant	Eligible Applicants: Fire departments, nonaffiliated EMS organizations; state fire training academies Competitive: 5% match is required	Personnel: Wellness and fitness programs for first responders Planning and Organization: Education on fire prevention and safety activities Training: Training materials Equipment: Protective gear, emergency vehicles, modification to facilities
DHS FEMA	Assistance to Firefighters Grant Fire Prevention and Safety (FP&S) FP&S grants support projects that enhance the safety of the public and firefighters from fire and related hazards. The primary goal is to reduce injury and prevent death among high-risk populations. http://www.fema.gov/fire-prevention-safety-grants	Eligible Applicants: Fire departments, national, regional, state, and local organizations, Tribal organizations, community organizations with fire prevention and/or fire safety expertise, private and public non-profit organizations Formula-based: Grantee cost sharing is 5% unless modified by a waiver	Planning and Organization: Education on fire prevention and safety activities Training: Training materials Equipment: Protective gear, emergency vehicles Research and Development: Topics include improving firefighter safety, health, or wellness through research and development that reduces firefighter fatalities and injuries
DHS FEMA	Emergency Management Performance Grant (EMPG) EMPG assists state, local and tribal governments in preparing for all hazards. EMPG provides granting funding to assist state emergency management agencies in obtaining the resources required to support the National Preparedness Goal's associated with Mission Areas and Core Capabilities. http://www.fema.gov/emergency-management-performance-grant-program	Eligible Applicants: State Administrative Agency (SAA) of states/territories or Emergency Management Agency (EMA); Grantee must belong to EMAC Eligible Sub-recipients: 100% of award is designated to the state-level EMA Formula-based: Amounts for each state/territory are listed in the NOFO; 50% match is required	Personnel: Staff to support management and administrative activities Planning and Organization: Engage emergency communications stakeholders in planning; coordinate activities focused on all-hazards management operations Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises Equipment: Cybersecurity enhancements, interoperable communications; maintenance and sustainment (e.g., upgrades, user fees, warranties); construction and renovation of communication towers

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
DHS FEMA	Transit Security Grant Program (TSGP) The TSGP directly supports transportation infrastructure security activities, and is one tool in the comprehensive set of measures to strengthen the Nation's critical infrastructure against risks associated with potential terrorist attacks. https://www.fema.gov/transit-security-grant-program	Eligible Applicants: Publicly owned operators of public transportation Competitive: Eligible transit agencies are determined based on daily unlinked passenger trips (ridership) and transit systems that serve historically eligible UASIs	Planning and Organization: Regional communications enhancement; governance integration Training: Develop, deliver, attend, and evaluate training Exercises: Develop, execute, and evaluate exercises Equipment: Related to interoperable communications, maintenance and sustainment, construction and renovation of communication towers
DHS FEMA	Port Security Grant Program (PSGP) The PSGP directly supports maritime transportation infrastructure security activities. PSGP is one tool to strengthen the Nation's critical infrastructure against risks associated with potential terrorist attacks. https://www.fema.gov/port-security-grant-program	Eligible Applicants: Port authorities, facility operators, and state/local government agencies Competitive: Port areas will be selected for funding through a competitive review process; Recipients must provide at least 25% match	Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises Equipment: Interoperable communications; upgrades, user fees, warranties; construction and renovation of communication towers and the Port Security Emergency Communications Center; enhance cybersecurity
DHS FEMA	Homeland Security Grant Program State Homeland Security Program (HSGP/SHSP) SHSP supports the implementation of risk driven, capabilities-based State Homeland Security Strategies to address capability targets set in urban area, state, and regional Threat and Hazard Identification Risk Assessments (THIRA). The capability targets are established during the THIRA process, and assessed in the State Preparedness Report, which inform planning, organization, equipment, training, and exercise needs to prevent, protect against, mitigate, respond to, and recover from acts of terrorism and other catastrophic events. https://www.fema.gov/homeland-security-grant-program	Eligible Applicants: SAAs of states/territories Eligible Sub-recipients: SAA must pass through 80% to local units of government Formula-based: Amounts for each state/territory are listed in the NOFO	Personnel: Staff to assist with management of respective grant program, application requirements, and compliance with reporting and data collection requirements; development of operating plans for information collection and processing necessary to respond to DHS/FEMA calls Planning and Organization: Statewide Interoperability Coordinator (SWIC) position, governance activities, communications plans, standard operating procedures, assessments Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises; implementation of HSEEP Equipment: Cyber security enhancements, interoperable communications; IT; maintenance and sustainment (e.g., upgrades, user fees, warranties); emergency supplies
DHS FEMA	Intercity Bus Security Grant Program (IBSGP) The IBSGP provides funding to owners and operators of intercity bus systems to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase the resilience of transit infrastructure. https://www.fema.gov/intercity-bus-security-grant-program	Eligible Applicants: Private operators providing transportation by an over-the-road bus in UASI jurisdiction Competitive: Eligible applicants must complete a vulnerability assessment and develop a security plan	Planning and Organization: Governance integration Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises Equipment: Cybersecurity enhancements, facility security; vehicle/driver security, construction and renovation of systems

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
DHS FEMA	Homeland Security Grant Program Urban Area Security Initiative (HSGP/UASI) The UASI program addresses the unique risk driven and capabilities-based planning, organization, equipment, training, exercise needs, of high-threat, high-density Urban Areas based on the capability targets identified during the THIRA process and associated assessment efforts, and assists them in building an enhanced and sustainable capacity to prevent, protect against, mitigate, respond to, and recover from acts of terrorism. https://www.fema.gov/homeland-security-grant-program	Eligible Applicants: SAA on behalf of eligible UASIs as listed in the NOFO Eligible Sub-recipients: SAA must pass through 80% to local units of government in the designated UASI Formula-based: Amounts for each jurisdiction are listed in the NOFO	Personnel: Staff to assist with management of respective grant program, application requirements, and compliance with reporting and data collection requirements; development of operating plans for information collection and processing necessary to respond to DHS/FEMA calls Planning and Organization: Statewide Interoperability Coordinator (SWIC) position, governance activities, communications plans, standard operating procedures, assessments Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises; implementation of HSEEP Equipment: Cyber security enhancements, interoperable communications; IT; maintenance and sustainment (e.g., upgrades, user fees, warranties); emergency supplies
DHS FEMA	Homeland Security Grant Program Operation Stonegarden (HSGP/OPSG) OPSG supports enhanced cooperation and coordination among local, tribal, territorial, state, and federal law enforcement agencies in a joint mission to secure the United States' borders along routes of ingress from international borders. This includes travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders. https://www.fema.gov/homeland-security-grant-program	Eligible Applicants: SAA on behalf of selected OPSG grantee Eligible Sub-recipients: SAA must pass through 100% to selected local units of government Competitive: States eligible to apply are listed in the NOFO	Personnel: Staff to assist with management of the respective grant program, application requirements, and compliance with reporting and data collection requirements; development of operating plans for information collection and processing necessary to respond to DHS/FEMA calls Planning and Organization: Coordination among jurisdictions, disciplines, various levels of governments (e.g., travel, per diem, overtime) Equipment: Interoperable communications; IT; emergency supplies
DHS FEMA	Non-Profit Security Grant Program (NSGP) The NSGP provides funding support for hardening and other physical security enhancements to non-profit organizations that are at high risk of a terrorist attack and located within one of the specific UASIs. https://www.fema.gov/nonprofit-security-grant-program	Eligible Applicants: SAA on behalf of non-profit organizations within eligible UASIs Eligible Sub-recipients: SAA must obligate 100% to selected nonprofit organizations Competitive: Non-profit organizations may receive funding following a competitive review process	Planning and Organization: Governance integration Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises Equipment: Cybersecurity, physical security and inspection/screening systems; construction and renovation

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
DHS Science & Technology Directorate	Small Business Innovation Research (SBIR) The SBIR program is a congressionally mandated small business set-aside designed to stimulate technological innovation and foster small business and private sector commercialization of innovations derived from federal Research and Development. http://www.dhs.gov/science-and-technology/sbir	Eligible Applicants: Small businesses, particularly small disadvantaged, women-owned, veteran-owned, service-disabled veteran-owned, and socially and economically disadvantaged small businesses Competitive: Each grant proposal will be evaluated on relevance of the specific concept as it relates to SBIR topics	Research and Development: Consist of topics relevant to the Borders and Maritime Security, Chemical/Biological Defense, Cyber Security, Explosives, Human Factors/Behavioral Sciences, and Infrastructure Protection and Disaster Management Divisions
Department of Health and Human Services (HHS)			
HHS Assistant Secretary for Preparedness and Response (ASPR)	Hospital Preparedness Program (HPP) The mission of HPP is to ready hospitals and other healthcare systems through enhanced surge capacity, capability, and in collaboration with other partners, to deliver coordinated and effective care to victims of terrorism and other public health emergencies, and improve community preparedness and resiliency. This cooperative agreement supports interoperable communications equipment, systems, training, and exercises. http://www.phe.gov/Preparedness/planning/hpp/Pages/funding.aspx	Eligible Applicants: States and territories, or a consortium of states Eligible Sub-recipients: Political subdivisions must submit a sufficient application to qualify Formula-based: Cooperative agreement is awarded to states or consortium of states with 10% matching requirement	Personnel: Staff to assist with planning, training, and exercises Planning and Organization: Engage emergency communications stakeholders in planning; develop assessments and inventories Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises Equipment: 911 activities and services related to emergency response efforts
HHS Center for Disease Control and Prevention (CDC)	Public Health Emergency Preparedness (PHEP) The purpose of the PHEP grant is to support and enhance the state and local public health infrastructure that is critical to public health preparedness and response. This grant supports interoperable communications equipment, systems, training, and exercises. http://www.cdc.gov/phpr/coopagreement.htm	Eligible Applicants: States and territories, or a consortium of states Eligible Sub-recipients: Political subdivisions must submit a sufficient application to qualify Formula-based: Cooperative agreement awarded to states or consortium of states with 10% matching requirement	Personnel: Staff to assist with planning, training, and exercises Planning and Organization: Engage emergency communications stakeholders in planning; develop assessments and inventories Training: Develop, deliver, attend, and evaluate training Exercises: Design, develop, execute, and evaluate exercises Equipment: 911 activities and services related to emergency response efforts

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
Department of Justice (DOJ)			
DOJ Community Oriented Policing Services (COPS)	Community Oriented Policing Services Coordinated Tribal Assistance Solicitation (COPS/CTAS) CTAS seeks to improve public safety and victim services in Tribal communities. The program provides federally-recognized Tribes and Tribal consortia an opportunity to develop a comprehensive and coordinated approach to public safety and victimization issues and to apply for funding. http://www.cops.usdoj.gov/Default.asp?Item=2489	Eligible Applicants: Federally-recognized Tribes or Tribal consortiums Competitive: Applications must focus on: enhance law enforcement, bolster justice systems, prevent youth substance abuse, address violence against women, serve crime victims, and support other efforts to combat crime	Personnel: Staff for technical assistance, law enforcement officers Training: Develop, deliver, attend, and evaluate training Equipment: Uniforms, basic issue equipment, technology, and vehicles
DOJ COPS	Community Oriented Policing Services Community Policing Development (COPS/CPD) CPD funds are used to advance the practice of community policing in law enforcement agencies through training and technical assistance, the development of innovative community policing strategies, applied research, guidebooks, and best practices that are national in scope. http://www.cops.usdoj.gov/default.asp?Item=2450	Eligible Applicants: Public government agencies, for-profit and nonprofit institutions, universities, community groups, and faith-based organizations Competitive: Awards or cooperative agreements granted to projects related to public safety topics	Personnel: Staff for project activities, contractors Training: Travel-related costs Equipment: Technology, supplies
DOJ Office of Justice Programs (OJP)	Edward Byrne Memorial Justice Assistance Grant Program (JAG) JAG funds support all components of the criminal justice system, from multi-jurisdictional drug and gang task forces to crime prevention and domestic violence programs, courts, corrections, treatment, and justice information sharing initiatives. https://www.bja.gov/ProgramDetails.aspx?Program_ID=59	Eligible Applicants: Local government units, which include a town, township, village, parish, city, county borough, or political subdivision of a state; federally-recognized Tribes; law enforcement district; judicial enforcement district established under state law Formula-based: JAG awards are based on a statutory formula in the NOFO	Personnel: Technical assistance, contractual support Planning and Organization: State and local initiatives Training: Develop and deliver trainings Equipment: Supplies, information systems for criminal justice Research and Development: Criminal justice-related research and evaluation activities

Agency / Office	Financial Assistance Program Description and Website	Eligibility and Allocation Method	Emergency Communications-Related Priorities and Allowable Costs
DOJ OJP/ National Institute of Justice (NIJ)	NIJ Research Grants in Law Enforcement, Geospatial, and Criminal Justice Information Technology NIJ awards grants and agreements for physical and social science research, development and evaluation projects about criminal justice through competitive solicitations, and two fellowships through annual solicitations. http://www.nij.gov/funding/current.htm	Eligible Applicants: Educational institutions, public agencies, non-profit organizations, faith-based organizations, individuals, profitmaking organizations willing to waive their fees, and federal agencies in the U.S. Eligible Sub-recipients: A U.S. grantee may subcontract with a non-U.S. institution or individual for work necessary to complete project tasks Competitive: Some solicitations have special eligibility criteria in the NOFO	Research and Development: Funds will support physical and social science research, development, and evaluation projects about criminal justice. The focus of the solicitations varies from year-to-year based on research priorities and available funding

4.3 POST AWARD

This section provides information on emergency communications technologies such as LMR, NG911, and broadband networks, and the status of public safety broadband projects nationwide. The tools include types of activities and key words that applicants may include in proposals, which will help federal program managers to identify specific projects that require additional review or guidance. Federal program managers are encouraged to use these tools to promote interoperability across federally-funded projects, as well as to mitigate risks associated with program funding.

4.3.1 Project 25 Activities and Key Words

Table 9 provides a list of LMR-related activities that support federal efforts to prepare for the deployment of P25 LMR networks. Federal program managers are encouraged to conduct a federal review of projects that contain any of the "Activity Types" or "Key Words" below to ensure proposed activities support the deployment of interoperable P25 systems.

Table 9. P25 Activities and Key Words

P25 Activities	
The public safety community partnered with the telecommunications industry to develop Project 25 (P25) standards for land mobile radio (LMR) systems. As a result, the Federal Government encourages the purchase of P25-compliant LMR equipment to ensure public safety systems can interoperate, regardless of manufacturer.	
Activity Types	**Key Words**
Planning for LMR Investments • Developing strategic plans or migration plans in preparation for a P25 implementation • Updating the Statewide Communication Interoperability Plan (SCIP) to incorporate P25 • Migration planning from legacy systems to other advanced technologies, including P25 systems engaging the whole community in planning • Assessing existing infrastructure • Hiring of personnel (e.g., Statewide Interoperability Coordinator [SWIC], project manager, technical experts) to develop plans for broadband deployment and to coordinate statewide efforts • Assessing costs for current services • Documenting current P25 providers • Contracts for termination dates and associated fees • Documenting the current "use case" information to develop outreach and education materials	• Planning for Project 25 • Survey existing infrastructure • Assessing existing LMR capabilities and assets • Development of cost maintenance models for equipment and usage • Hiring of Radio Frequency (RF) engineers or Enterprise Architects to assist with planning

Analysis/Transition of existing LMR systems • Updating existing system to P25 Conventional • Updating existing system to P25 Trunking • Developing a system migration plan from legacy LMR system to P25	• Analysis/Assessment of existing narrowband LMR systems that have already deployed for public safety • Migrating of current narrowband systems operating in the public safety spectrum • Very high frequency (VHF), ultra-high frequency (UHF), 700 / 800 megahertz (MHz) • RF engineering • Transition/migration planning and execution • Security Services
Site Upgrades • Documenting and/or upgrading existing site capabilities • Installing/expanding battery backup, generators, or fuel systems • Evaluating existing shelter space for the inclusion of new equipment • Conducting tower loading analysis to determine feasibility of supporting new antennas and equipment • Analyzing site power and grounding systems to determine upgrades needed to support additional communications equipment • Analyzing physical site security provisions to determine upgrades and enhancements (e.g., fences, lighting, alarms, cameras)	• Site upgrades • Battery backup • Generators • Shelters • Tower analysis • 700 / 800MHz antennas • Analysis of site power/grounding
Backhaul - projects focused on upgrading connectivity capabilities for public safety communications • Documenting existing wireline/wireless backhaul resources to determine used and excess capacity (e.g., connectivity type [i.e., fiber, wireline, cable] at existing public safety facilities, including Public Safety Answering Points [PSAP]) • Analyzing existing Internet-Protocol (IP) backbone to determine gaps in supporting high bandwidth public safety communication systems • Planning and modeling network capacity to ensure backhaul links and aggregation points are appropriately provisioned • Upgrading existing backbone to support advanced capabilities (e.g., multi-protocol line switching [MPLS]) • Installing fiber optic connections to support enhanced communications and networking capabilities • Assessing and documenting the usage of wireless communications capabilities (e.g., mobile data systems, applications, devices, gaps) • Assessing high bandwidth data capabilities • Installing sufficient microwave connectivity to support enhanced communications and network capabilities	• Assessment of wireline or wireless backhaul • Assessment of connectivity type (i.e., fiber, wireline, cable) • Assessment of existing PSAP fiber capacity • Network capacity planning/modeling • Backbone upgrades • Installation of fiber optic connections to support data capabilities • Installation of microwave connectivity • Analysis of IP backbone

Ancillary equipment • Land mobile radio test equipment such as handheld spectrum analyzers, cable testers, and drive test tools	• LMR test equipment • Handheld spectrum analyzers • Cable testers • Drive test tools
Project 25-related investments • Federal program managers and staff can use key words to the right to identify Project 25-related investments that should be submitted for federal review	• VHF / UHF • P25 Compliance Assessment Program (CAP) • Open architecture standards • Enhanced interoperability • Secure communications • TIA-102 • P25 Statement of Requirements (SoR) • Legacy systems • Advanced Digital Protection (ADP)
Design of LMR Network • Project 25 systems involving system design should be flagged for review to ensure they comply with the most current standards	• TIA-102 Project 25 Suite of Standards • As-is and proposed enterprise architectures • Hiring of RF Engineers/Enterprise Architects/Network Planners to assist with design or implementation
Acquisition • Acquisition of equipment capable of operating in the public safety bands may indicate a mission critical project; examples of equipment are provided in the column on the right and should be flagged for review	• P25 equipment • Radio equipment devices/handsets • VHF, UHF, 700 / 800 MHz • Security Services • Legacy systems • Advanced Digital Protection (ADP) • Over the air programming (OTAP) • Over the air rekeying (OTAR) • Independent verification and validation (IV&V)
Implementation • Deployment or implementation of a P25 network should be flagged for review to ensure compliance with the most current standards	• Construction of VHF, UHF, 700 / 800 MHz system • Security Services • Enhanced interoperability
Operations • Projects that reference operational costs (e.g., user fees) may indicate a lease-to-own project and should be flagged for review	• User/subscriber fees • Reimbursement of cellular/ satellite user fees
Capabilities associated with LMR • Project capabilities associated with non-standard LMR technologies should be flagged for review	• Video • High Definition • Streaming • Data-sharing • High-speed data transmission • OTAP • MotoTRBO • Nextedge • Smartnet • SmartZone • ADP

4.3.2 Next Generation 911 Activities and Key Words

Federal program managers are encouraged to conduct a federal review of projects that contain any of the "Activity Types" or "Key Words" in Table 10 to ensure proposed activities support the deployment of interoperable 911 systems or NG911. Federal program managers may also contact the ECPC GFG for clarification, additional guidance, or subject matter-level review of NG911 activities.

Table 10. NG911 Activities and Key Words

NG911 Activities	
Next Generation 911 (NG911) is an Internet Protocol (IP)-based system that allows digital information (e.g., voice, photos, videos, text messages) to flow seamlessly from emergency callers to public safety answering points (PSAPs) and on to emergency responders.	
Activity Types	**Key Words**
Governance • Identifying and designating personnel (e.g., Statewide Interoperability Coordinator [SWIC], project manager, technical experts) to coordinate local and/or statewide NG911 efforts • Establishing or managing a governance body or working group (e.g., Statewide Interoperability Executive Committee [SIEC], State 911 Office, State 911 Board) designated to address NG911 planning • Establishing governance documents and agreements (e.g. Memorandum of Understanding [MOU]) • Developing documents to advise authorities on designing the Emergency Services IP networks (ESInets), core NG911 infrastructure, and connectivity PSAPs	• Hiring of Information Technology experts to assist with NG911 planning • Building or expanding governance structures to include 911 leaders • Integrating 911 leadership and governance structures into broader statewide planning efforts • Defining key roles and responsibilities for entities involved in NG911 planning and deployment
Planning and Outreach • Developing a StateNG911 Plan, NG911 Strategic Plan, and updating the Statewide Communication Interoperability Plan (SCIP)in preparation for NG911 implementation • Developing an NG911 Feasibility Study assessing regional solutions and cost models for NG911 transition • Conducting analysis for NG911 vendors and service offerings • Developing a system roadmap from legacy 911 or Enhanced 911 (E911) system to NG911 • Developing outreach and education materials for the 911 community, emergency responders, and the general public (e.g., ability to transmit text messages, video, or data to 911 and to assist emergency responders)	• Analysis/assessment of existing NG911 systems that have already been deployed for public safety • Planning for IP-enabled Next Generation 911 or NG911 • Survey of 911 infrastructure • Contingency Plans • Assessment of existing PSAP capabilities and assets • Development of cost maintenance models for 911 equipment and usage • Migration of legacy or Enhanced 911 systems • Transition/migration planning and execution for NG911 • NG911 outreach materials (e.g., flyers, videos, public service announcements [PSA])

Policies and Operations • Establishing operating policies and agreements for operating NG911 (e.g., Memoranda of Understanding [MOU], Standard Operating Procedures [SOP]) • Drafting procedures for identifying and correcting NG911 geographic data discrepancies at local, regional, state, and national levels • Developing cybersecurity policies and procedures for handling, storing, and safe-guarding NG911 data and networks • Ensuring that geospatial data and geographic routing or location validation databases meet quality assurance standards • Developing procedures to reconcile legacy location validation and routing databases to NG911 Geographic Information Systems (GIS)-based databases	• Call Routing • Emergency Services IP networks (ESInets) • Maintenance of ESInets and other infrastructure • Geographic Information Systems (GIS) Data • NG911 Core Services • Quality Assurance of networks and operations • Contracts between providers, PSAPs, and other public safety entities • Service Routing Issues • Telematics • Security services

4.3.3 Broadband Activities and Key Words

Federal program managers are encouraged to review the allowable broadband activities for the deployment of the NPSBN as listed in Table 11, as well as the "high risk" broadband activities that are subject to review in Table 12. These activities may qualify for federal funding as they relate to emergency communications.

While entities may want to pursue funding for broadband equipment and systems, ther limited equipment available may not comply with FirstNet's final network architecture and be able to integrate into the NPSBN. Therefore, federal program managers should advise applicants to plan for a long-term evolution (LTE) and delay acquisition of LTE equipment until there is further guidance from FirstNet; rather, stakeholders should target funding toward allowable broadband activities.

Table 11. Allowable Broadband Activities and Key Words

Allowable Broadband Activities	
State and local public safety agencies are coordinating with FirstNet and preparing for the deployment of the nationwide public safety broadband network (NPSBN). While FirstNet develops the NPSBN network architecture requirements, public safety agencies may plan for broadband investments by conducting activities in the following five categories.	
Activity Types	**Key Words**
Category 1: Planning for Broadband Investments • Developing strategic plans or migration plans in preparation for participation in a 700 megahertz (MHz) NPSBN • Updating the Statewide Communication Interoperability Plan (SCIP) to incorporate broadband planning • Migration planning from legacy systems to other advanced technologies, including broadband systems engaging the whole community in planning • Assessing existing infrastructure • Hiring of personnel (e.g., Statewide Interoperability Coordinator • [SWIC], project manager, technical experts) to develop plans for broadband deployment and to coordinate statewide efforts • Assessing costs for current services • Documenting current broadband providers • Contracts for termination dates and associated fees • Documenting the current "use case" information to develop outreach and education materials	• Planning for broadband • Broadband assessments • Survey existing infrastructure • Assessing existing broadband capabilities and assets • Development of cost maintenance models for equipment and usage • Hiring of Radio Frequency (RF) engineers or Enterprise Architects to assist with planning • Agency on-boarding (e.g. IT infrastructure upgrades)

Category 2: Analysis/Transition of existing narrowband land mobile radio (LMR) systems that have already deployed in the public safety broadband spectrum • Rebanding of currently deployed LMR 700 MHz narrowband systems within the public safety broadband spectrum allocation to the authorized 700 MHz narrowband allocation	• Analysis/Assessment of existing narrowband LMR systems that have already deployed in the public safety broadband allocation • Rebanding or migrating of current narrowband systems operating in the 700 MHz public safety broadband spectrum • RF engineering • Transition/migration planning and execution
Category 3: Site Upgrades • Documenting and/or upgrading existing site capabilities • Installing/expanding battery backup, generators, or fuel systems • Evaluating existing shelter space for the inclusion of new equipment • Conducting tower loading analysis to determine feasibility of supporting new antennas and equipment • Analyzing site power and grounding systems to determine upgrades needed to support additional communications equipment • Analyzing physical site security provisions to determine upgrades and enhancements (e.g., fences, lighting, alarms, cameras)	• Site upgrades • Battery backup • Generators • Shelters • Tower analysis • 700 MHz antennas • Analysis of site power/grounding • Broadband IP-based backhaul
Category 4: Backhaul projects focused on upgrading connectivity capabilities for public safety broadband • Documenting existing wireline/wireless backhaul resources to determine used and excess capacity (e.g., connectivity type [i.e., fiber, wireline, cable] at existing public safety facilities, including public safety answering points) • Analyzing existing Internet-Protocol (IP) backbone to determine gaps in supporting high bandwidth public safety communication systems • Planning and modeling network capacity to ensure backhaul links and aggregation points are appropriately provisioned • Upgrading existing backbone to support advanced capabilities (e.g., multi-protocol line switching [MPLS]) • Installing fiber optic connections to support enhanced communications and networking capabilities • Assessing and documenting the usage of wireless communications capabilities (e.g., mobile data systems, applications, devices, gaps) • Assessing high bandwidth data capabilities • Installing sufficient microwave connectivity to support enhanced communications and network capabilities	• Assessment of wireline or wireless backhaul • Assessment of connectivity type (i.e., fiber, wireline, cable) • Assessment of existing PSAP fiber capacity and potential alignment • Network capacity planning/modeling • Backbone upgrades • Installation of fiber optic connections to support data capabilities • Installation of microwave connectivity • Analysis of IP backbone
Category 5: Ancillary equipment • Long-term Evolution (LTE) test equipment such as handheld spectrum analyzers, cable testers, and drive test tools • Cellular on wheel/cellular on light truck (COW/COLT) capabilities	• LTE test equipment • Handheld spectrum analyzers • Cable testers • Drive test tools • COW/COLT capabilities

Table 12. Broadband Activities Subject to Review

Broadband Activities Subject to Review	
Public safety agencies are strongly advised to delay acquisition of long-term evolution (LTE) network equipment in the following six categories pending further guidance from FirstNet on the technical requirements of the NPSBN and to continue to target funding toward planning activities (e.g., community outreach and education, documenting user needs) and support statewide planning for the eventual arrival of broadband and other advanced technologies.	
Activity Types	**Key Words**
Category 1: Wireless Broadband-related investments • Federal program managers and staff can use key words to the right to identify broadband-related investments that should be submitted for federal review	• Wireless Broadband • RAN (Radio Access Network) • Long-term Evolution (LTE) • Wi-Fi • 3G/4G/5G • 700 MHz public safety band • D Block • Nationwide Public Safety Broadband Network (NPSBN) • FirstNet • Add-ons to Broadband Technology Opportunities Program (BTOP) or Broadband Initiatives Program (BIP) projects • Advanced technology/innovative/cutting-edge • Projects proposing to operate in the T-band • Projects that cite participation in a 700 MHz Broadband Demonstration Network
Category 2: Design of Wireless Radio Access Networks (RAN) • Activities to implement the NPSBN are still under development, including system requirements; therefore, projects involving system design should be flagged for review to ensure they comply with the most current requirements developed by FirstNet	• LTE/RAN (broadband) systems design • LTE/RAN (broadband) equipment planning and design • Developing system engineering requirements for a LTE wireless RAN systems • As-is and proposed enterprise architectures • Hiring of RF Engineers/Enterprise Architects/Network Planners to assist with design or implementation
Category 3: Acquisition • Acquisition of equipment capable of operating in the 700 MHz public safety band may indicate a broadband-related project; examples of equipment are provided in the column on the right and should be flagged for review	• LTE RAN equipment • Cloud RANs • LTE equipment 700 MHz LTE devices/handsets • Band 14 capable equipment • Purchase of equipment for use with the 700 MHz public safety broadband wireless network (i.e., 700 MHz-capable mobile, portable, infrastructure equipment) • Hosted Core • Evolved Packet Core (EPC) • eNodeB equipment • Small cells (femtocells, picocells) • Distributed Antenna Systems (DAS) • Opt-out

Category 4: Implementation • Deployment or implementation of a broadband network should be flagged for review to ensure compliance with the most current requirements developed by FirstNet for the NPSBN	• Construction of 700 MHz Wireless LTE broadband network • Spectrum sharing • Carrier aggregation • Cloud computing/hosting • Mobile Virtual Network Operation (MVNO) • Agency on-boarding (e.g. cloud hosting subscription fees)
Category 5: Operations • Projects that reference operational costs (e.g., user fees) may indicate a broadband-related project and should be flagged for review	• User/subscriber fees • Secondary users • Reimbursement of cellular/ satellite user fees • Roaming to commercial networks • Public/private partnerships
Category 6: Capabilities associated with broadband • The key words listed on the right are capabilities associated with broadband networks; projects that include any of these capabilities should be flagged for review	• Video • High Definition • Streaming • Data-sharing • High-speed data transmission • On-line access to blueprints • Voice over LTE • Mobile applications (Apps) • Computer Aided Dispatch (CAD) systems • Situational Awareness Applications • Agency applications (e.g. records management, email) • Location-based services • Near Field Communication (NFC) • Machine-to-Machine (M2M) Communication • Agency on-boarding (e.g. IT infrastructure upgrades) • Big data analytics

4.3.4 Status of Public Safety Broadband Projects

Federal program managers are encouraged to review the jurisdictions currently licensed to operate on the combined public safety broadband spectrum band (763-768 MHz and 793-798 MHz) and D Block spectrum (758-763 MHz and 788-793 MHz), also referred to as Band 14, as provided in Table 13. FirstNet has granted Spectrum Management Lease Agreements (SMLA) to five projects for their use of Band 14 spectrum. FirstNet does not anticipate awarding any more SMLAs prior to the deployment of the NPSBN.

Applicants submitting proposals for broadband deployment activities must have authority to operate in the 700 MHz public safety spectrum. Entities that do not have authority to operate in this spectrum should not receive funding for broadband deployment activities. However, all jurisdictions may be eligible to fund broadband planning activities (e.g., community outreach and education, documenting user needs).

Table 13. Status of Public Safety Broadband Projects

<table>
<tr><th colspan="4">Background</th></tr>
<tr><td colspan="4">

In May 2010, the FCC issued conditional waivers allowing 21 petitioners to deploy broadband systems in the 700 MHz band. The Broadband Technology Opportunities Program (BTOP) awarded funding to seven of the waiver recipients.
In February 2012, the Middle Class Tax Relief and Job Creation Act authorized the establishment of a NPSBN, required the transfer of the public safety spectrum to FirstNet, and appointed FirstNet to serve as the single licensee and operator of the network.
In November 2012, the FCC issued the license to FirstNet. FirstNet began working with BTOP recipients and Harris County, TX (a non-BTOP recipient) to develop lease agreements.
In 2013 and 2014, four BTOP recipients and Harris County, TX were able to sign a lease agreement with FirstNet for the use of the 700 MHz public safety spectrum.
All previous 700 MHz waiver recipients and the three BTOP recipients unable to come to an agreement with FirstNet do not have access to the 700 MHz public safety spectrum.

</td></tr>
<tr><th colspan="2">700 MHz Waiver Recipients</th><th>BTOP Recipients</th><th>FirstNet Lease Agreements</th></tr>
<tr>
<td colspan="2">
States (8)

Hawaii
Iowa
Mississippi
New Jersey
New Mexico
New York
Oregon
Texas

Counties/Regions (5)

Adams County, CO
Bay Area, CA
Los Angeles, CA
Mesa-TOPAZ, AZ
Wisconsin Counties, WI

Cities (8)

Boston, MA
Charlotte, NC
Chesapeake, VA
Pembroke Pines, FL
New York City, NY
San Antonio, TX
Seattle, WA
Washington, DC

</td>
<td>

New Jersey
New Mexico
Mississippi
Adams County, CO
Bay Area, CA
Los Angeles, CA
Charlotte, NC

</td>
<td>

Los Angeles, CA (June 27, 2013)
New Mexico (July 23, 2013)
New Jersey (Dec 17, 2013)
Adams County, CO (Dec 17, 2013)
Harris County, TX (Aug 15, 2014)

</td>
</tr>
</table>

4.4 CLOSEOUT

This section supports federal program managers in completing the closeout reporting requirements of a program. As the grant cycle ends, recipients may use various programmatic procedures and financial forms to report their emergency communications-related expenditures. While specific reporting requirements may vary, the ECPC GFG recommends that federal program managers gather data that would demonstrate the impact of funding on emergency communications activities.

4.4.1 ECPC GFG Data Collection Template

Federal agencies are under pressure to demonstrate the impact and effectiveness of financial assistance programs. To help federal program managers more easily identify and report on emergency communications projects and funding, the ECPC GFG has developed a template to help federal program managers analyze and report on the emergency communications-specific data elements in Table 14. This data collection will also help the ECPC GFG assess the level and impact of federal financial assistance on emergency communications nationwide.

Table 14. ECPC GFG Data Collection Template

Program Name	Fiscal Year	Total Program Funds	Number of EC Projects	Total Funding for EC Projects	Subtotal of EC Funding spent on Equipment
Example Project	2015	$306,022,500	61	$6,242,627	$3,136,067

**EC is an abbreviation for emergency communications-related activities.*

Emergency Communications Preparedness Center

ECPC Grants Focus Group Overview

The Emergency Communications Preparedness Center (ECPC) is the federal interagency focal point for interoperable and operable emergency communications coordination. The ECPC Grants Focus Group (GFG) was charged to develop common guidance for federal programs that support emergency communications financial assistance programs. Comprised of grants officers, program administrators, and communications experts, the ECPC GFG has representation from eight federal departments and agencies including:

ECPC Member Departments and Agencies

- **U.S. Department of Agriculture***
- **General Services Administration**
- **U.S. Department of Labor**
- **U.S. Department of Commerce***
- **U.S. Department of Health and Human Services***
- **U.S. Department of State**
- **U.S. Department of Defense**
- **U.S. Department of Homeland Security***
- **U.S. Department of Transportation***
- **U.S. Department of Energy**
- **U.S. Department of the Interior***
- **U.S. Department of the Treasury**
- **Federal Communications Commission***
- **U.S. Department of Justice***

Denotes ECPC Grants Focus Group Member

ECPC GFG Priorities

To implement the ECPC charge to develop common guidance for federal programs, the ECPC GFG developed a strategic approach comprised of three priorities that drive the group's and its member agencies' activities:

1) Promote consistency in policy across federal financial assistance programs that fund emergency communications;
2) Coordinate across federal agencies and financial assistance programs to support the advancement of emergency communications; and
3) Improve the understanding of emergency communications funding

ECPC GFG Resources

The ECPC GFG offers the following resources to support federal program managers:

- Membership meetings to discuss issues impacting the federal financial assistance community
- *ECPC Recommendations for Federal Agencies*, sets the national strategy for federal financial assistance programs that fund emergency communications—including grants, loans, and cooperative agreements
- *ECPC Federal Financial Assistance Reference Guide*, designed for federal program managers to understand emergency communications issues and to recommend best practices for developing, implementing, and evaluating emergency communications activities
- *SAFECOM Guidance on Emergency Communications Grants* (www.dhs.gov/safecom), updated annually for grantees applying for emergency communications funding, to provide grantees the latest policy requirements, best practices, and technical standards from partnering federal agencies
- Programmatic review tools to assist federal program managers recognize and mitigate risks related to emergency communications technologies, including FirstNet requirements for wireless broadband, Next Generation 911 network migration, and Project 25 standards for land mobile radio systems
- Points of contact for interagency coordination
- ECPC Clearinghouse (www.max.gov) to share intergovernmental information relating to emergency communications. All ECPC GFG resources are available following website registration and access request

For more information on the ECPC or emergency communications issues, please contact ecpc@hq.dhs.gov