Preparedness Grants Manual

FM-207-23-001

August 2025

FEMA

This page intentionally left blank

Table of Contents

1. **Foreword** **5**
   - 1.1. Overview of the Preparedness Grants Manual's Intent 5
   - 1.2. Key Changes 5
   - 1.3. Overview of Preparedness Grant Programs 6
   - 1.4. National Preparedness Goal 8
   - 1.5. Strengthening Governance Integration 9
2. **Award Determination and Obligation** **11**
   - 2.1. Federal Award Administration Information 11
3. **Recipient and Subrecipient Costs** **12**
   - 3.1. General Funding Requirements 12
   - 3.2. Direct Allowable Costs 12
   - 3.3. Maintenance and Sustainment 15
   - 3.4. Management and Administration 16
   - 3.5. Procedures for Establishing Indirect Cost Rates 17
4. **Administrative and National Policy Requirements** **18**
   - 4.1. Presidential Executive Orders 18
   - 4.2. Subrecipient Monitoring and Management 18
   - 4.3. Accessibility Compliance 18
   - 4.4. Adaptive Support 18
   - 4.5. Environmental Planning and Historic Preservation Compliance 19
   - 4.6. Domestic Preferences for Procurement 20
   - 4.7. Financial Assistance Programs for Infrastructure 21
   - 4.8. Davis-Bacon Act Compliance 21
   - 4.9. National Incident Management System Implementation 21
   - 4.10. SAFECOM Guidance Compliance 22
   - 4.11. Resilient Communications Guidance 24
   - 4.12. FirstNet 25
   - 4.13. Department of Homeland Security/FEMA Communications Support Services 26
5. **Post-Award Management and Implementation** **29**

5.1. Reporting 29
5.2. Federal Financial Reporting Requirements 29
5.3. Program Performance Reporting Requirements 30
5.4. Biannual Strategy Implementation Report 31
5.5. Closeout Reporting Requirements 31
5.6. Administrative Closeout 32
5.7. Disclosing Information per 2 C.F.R. § 180.335 32
5.8. Reporting of Matters Related to Recipient Integrity and Performance 33
6. Additional Information 34
6.1. Monitoring and Oversight 34
6.2. Case Studies and Use of Grant-Funded Resources During Real-World Incident Operations 37
6.3. Termination of the Federal Award 38
6.4. Period of Performance Extensions 40
6.5. Conflicts of Interest in the Administration of Federal Awards or Subawards 41
6.6. Procurement Integrity 41
6.7. Records Retention 43
6.8. Actions to Address Noncompliance 44
6.9. Audits 44
6.10. Reporting Issues of Fraud, Waste, and Abuse 45
6.11. Payment Information 45
6.12. Whole Community Preparedness 46
7. Resources 48
7.1. Department of Homeland Security/FEMA Provided Training and Education 48
7.2. Training Not Provided by the Department of Homeland Security/FEMA 48
7.3. Training Information Reporting System (“Web-Forms”) 48
7.4. FEMA’s National Preparedness Course Catalog 49
7.5. Exercises 49
7.6. Planning Assistance 49
7.7. Training Information 49
7.8. Weblinks 50

7.9. Emergency Management Accreditation Program 50

8. Homeland Security Grant Program and Tribal Homeland Security Grant Program 51

8.1. Alignment to the National Preparedness System (Homeland Security Grant Program, Tribal Homeland Security Grant Program) 51

8.2. Reporting on the Implementation of the National Preparedness System (Homeland Security Grant Program, Tribal Homeland Security Grant Program) 52

8.3. Funding Guidelines (Homeland Security Grant Program, Tribal Homeland Security Grant Program) 55

8.4. Allowable Cost (Homeland Security Grant Program) 55

8.5. Fusion Centers (Homeland Security Grant Program) 56

8.6. Investment Modifications – Changes in Scope or Objective (Tribal Homeland Security Grant Program) 60

8.7. Continuity Capability (Homeland Security Grant Program, Tribal Homeland Security Grant Program) 61

8.8. Senior Advisory Committee (Homeland Security Grant Program) 61

8.9. Urban Area Working Group (Homeland Security Grant Program) 64

8.10. Supplemental State Homeland Security Program and Urban Area Security Initiative Guidance (Homeland Security Grant Program) 66

8.11. Operation Stonegarden Operational Guidance (Homeland Security Grant Program) 67

8.12. Pass-Through Requirements (Homeland Security Grant Program) 75

8.13. Supplemental Resources (Homeland Security Grant Program, Tribal Homeland Security Grant Program) 77

9. Nonprofit Security Grant Program 80

9.1. Program Funding Guidelines and Priorities 80

9.2. Nonprofit Security Grant Program Investment Modifications – Changes in Scope or Objective 80

9.3. Pass-Through Requirements 81

10. Surface Transportation Security Grant Programs (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program) 83

10.1. Program Funding Guidelines and Priorities (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program) 83

10.2. Changes in Scope or Objectives (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program) 83

10.3. Security Plan Requirements (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program) 83

10.4. Allowable Cost Guidance 86

11. Port Security Grant Program 88

11.1. Program Funding Guidelines and Priorities 88

11.2. Allowable Cost Guidance 88

11.3. Port-Wide Risk Management Plans 90

11.4. Port Security Grant Program Investment Modifications 90

12. Emergency Management Performance Grant Program 92

12.1. Alignment of the Emergency Management Performance Grant Program to the National Preparedness System 92

12.2. Implementation of the National Preparedness System 93

12.3. Logistics Planning 97

12.4. Evacuation Planning 98

12.5. Disaster Housing Planning 99

12.6. State Disaster Recovery Coordinator 99

12.7. Disaster Financial Management Policies and Procedures 100

12.8. Training and Exercises 102

12.9. Reviewing and Updating Planning Products 106

12.10. Program Performance Reporting Requirements 106

13. Abbreviations and Acronyms 108

1. Foreword

1.1. Overview of the Preparedness Grants Manual's Intent

The Federal Emergency Management Agency developed this **Preparedness Grants Manual** to guide grant recipients, including subrecipients, on how to manage their grants. Recipients seeking guidance on policies and procedures for managing FEMA preparedness grants should reference this manual. The Notice of Funding Opportunity (NOFO) for each preparedness grant program includes information needed to apply for that grant. This manual and relevant NOFOs can be reviewed and consulted in tandem.

Chapters 8-12 of this manual contain program-specific information and requirements, while the main content of this manual (chapters 1-7) contains important information relevant to all preparedness grant programs unless otherwise noted. Please be sure to read both the main content of this manual as well as the program-specific chapters as needed.

All recipients and subrecipients of FEMA grants must comply with all applicable requirements of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards located at 2 C.F.R. Part 200. For more information on 2 C.F.R. Part 200, please see Information Bulletin (IB) 400, FEMA's Implementation of 2 C.F.R. Part 200, the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards ("Super Circular" or "Omni Circular") dated Dec. 23, 2014, regarding FEMA's implementation of these provisions before the recent 2020 and 2024 revisions. For information on the recent revisions to these regulations, see 2 C.F.R. Grants Management Policy Updates.

1.2. Key Changes

Several sections of the manual received new or refreshed content for Fiscal Year (FY) 2025, mainly to align with updated standard language included across FEMA's FY 2025 NOFOs. Impacted sections include:

- 2.1.1 Notice of Award
- 3.1 General Funding Requirements
- 3.2.3 Prohibition on Covered Equipment or Services
- 4.1 Presidential Executive Orders
- 4.2 Subrecipient Monitoring and Management
- 4.4 Adaptive Support
- 4.5 Environmental Planning and Historic Preservation Compliance
- 46 Financial Assistance Programs for Infrastructure
- 5.2 Federal Financial Reporting Requirements
- 5.5 Closeout Reporting Requirements

- 5.6 Administrative Closeout
- 5.7 Disclosing Information per 2 C.F.R. § 180.335
- 5.8 Reporting of Matters Related to Recipient Integrity and Performance
- 6.3 Termination of the Federal Award
- 6.6 Procurement Integrity
- 6.8 Records Retention
- 6.9 Actions to Address Noncompliance
- 6.10 Audits

Additional key changes were made to the following sections:

- Updated Sections 3.2.1 Authorized Equipment List and 3.2.2 Requirements for Small Unmanned Aircraft Systems to remove content related to prohibited and controlled equipment.
- Updated Section 3.2.2 Requirements for Small Unmanned Aircraft Systems to include information on an upcoming prohibition on covered unmanned aircraft systems from covered foreign entities.
- Added 4.6 Domestic Preferences for Procurement to reflect an administration priority about purchasing, acquiring, or using goods, products, or materials produced in the United States.
- Updated Section 6.12 Payment Information to include new requirements related to review of payment requests.
- Updated Section 8.11 Operation Stonegarden Operational Guidance to remove requirement to develop a Concept of Operations.
- Added Section 8.12 Pass-Through Requirements to capture HSGP pass-through requirements that were previously included in the NOFO.

1.3. Overview of Preparedness Grant Programs

FEMA has the statutory authority to deliver numerous disaster and non-disaster (ND) financial assistance programs in support of its mission, and that of the U.S. Department of Homeland Security (DHS), largely through grants and cooperative agreements. These programs account for a significant amount of the federal assistance funds for which FEMA is accountable. FEMA officials are responsible and accountable for the proper administration of these funds pursuant to federal laws and regulations, Office of Management and Budget (OMB) circulars, and federal appropriations laws and principles. FEMA developed this manual to provide uniform direction on grant policy and implementation for the following grant programs. If the FEMA grant program you are looking for is not listed below, please navigate to FEMA.gov to find more information.

1.3.1. HOMELAND SECURITY GRANT PROGRAM

The Homeland Security Grant Program (HSGP) includes a suite of risk-based grants to assist state, local, tribal, and territorial (SLTT) efforts in preventing, preparing for, protecting against, and responding to acts of terrorism. The grants under HSGP include:

- State Homeland Security Program (SHSP): SHSP assists SLTT efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.
- Urban Area Security Initiative (UASI): The UASI assists high-risk urban areas' efforts to build, sustain, and deliver the capabilities necessary to prevent, prepare for, protect against, and respond to acts of terrorism.
- Operation Stonegarden (OPSG): OPSG supports enhanced cooperation and coordination among U.S. Customs and Border Protection (CBP), United States Border Patrol (USBP), and federal and SLTT law enforcement agencies to improve overall border security. OPSG provides funding to support joint efforts to secure U.S. borders along routes of ingress/egress to and from international borders, to include travel corridors in states bordering Mexico and Canada, as well as states and territories with international water borders. SLTT law enforcement agencies utilize their own law enforcement authorities to support the border security mission and do not receive any additional authority by participating in OPSG.

For additional information about the HSGP not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-Grants-News@fema.dhs.gov.

1.3.2. TRIBAL HOMELAND SECURITY GRANT PROGRAM

The Tribal Homeland Security Grant Program (THSGP) provides funding directly to eligible Tribal Nations to strengthen their capacity to prevent, prepare for, protect against, and respond to potential terrorist attacks.

- For additional information about the THSGP not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-THSGP@fema.dhs.gov.

1.3.3. NONPROFIT SECURITY GRANT PROGRAM

The Nonprofit Security Grant Program (NSGP) provides funding for physical and cybersecurity enhancements and other security-related activities to nonprofit organizations that are at high risk of a terrorist or other extremist attack. The NSGP also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts.

- For additional information about the NSGP not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-NSGP@fema.dhs.gov.

1.3.4. TRANSIT SECURITY GRANT PROGRAM

The Transit Security Grant Program (TSGP) provides funds to eligible public transportation systems (which include intra-city bus, ferries, and all forms of passenger rail) to protect critical transportation infrastructure and the travelling public from terrorism, and to increase transportation infrastructure resilience.

- For additional information about the TSGP not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-TISB-rail-and-transit@fema.dhs.gov.

1.3.5. INTERCITY BUS SECURITY GRANT PROGRAM

The Intercity Bus Security Grant Program (IBSGP) provides funds to eligible private operators of intercity over-the-road buses to protect critical transportation infrastructure and the travelling public from acts of terrorism, and to increase transportation infrastructure resilience.

- For additional information about the IBSGP not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-TISB-rail-and-transit@fema.dhs.gov.

1.3.6. INTERCITY PASSENGER RAIL PROGRAM - AMTRAK

The Intercity Passenger Rail (IPR) Program provides funds to the National Railroad Passenger Corporation (Amtrak) to protect critical transportation infrastructure and the travelling public from terrorism, and to increase transportation infrastructure resilience.

- For additional information about the IPR Program not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-TISB-rail-and-transit@fema.dhs.gov.

1.3.7. PORT SECURITY GRANT PROGRAM

The Port Security Grant Program (PSGP) provides funding to port authorities, facility operators, and state and local agencies for activities associated with implementing Area Maritime Security Plans (AMSP), facility security plans, and other port-wide risk management efforts.

- For additional information about the PSGP not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-GPD-PSGP@fema.dhs.gov.

1.3.8. EMERGENCY MANAGEMENT PERFORMANCE GRANT PROGRAM

The Emergency Management Performance Grant (EMPG) Program provides funds to assist SLTT emergency management agencies in obtaining the resources required for implementation of the National Preparedness System and the National Preparedness Goal of a secure and resilient nation.

- For additional information about the EMPG Program not found in the NOFO, this manual, or other program-specific guidance, contact FEMA-EMPG@fema.dhs.gov.

1.4. National Preparedness Goal

The National Preparedness Goal (the Goal) 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 Goal essentially defines what it means for all communities to be prepared collectively for the threats and hazards that pose the greatest risk to the nation. The Goal identifies 32 distinct activities, called core capabilities, needed to address the risks. The Goal organizes these core capabilities into five categories, called mission areas. Some core capabilities apply to more than one mission area. For example, the first three core capabilities—Planning, Public Information and Warning, and Operational Coordination—are cross-cutting capabilities, meaning they apply to each of the five mission areas. The Goal's five mission areas include:

- **Prevention**: Prevent, avoid, or stop an imminent, threatened, or actual act of terrorism.
- **Protection**: Protect our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive.
- **Mitigation**: Reduce the loss of life and property by lessening the impact of future disasters.
- **Response**: Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of an incident.
- **Recovery**: Recover through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by an incident.

The mission areas and core capabilities organize the activities and tasks performed before, during, and after disasters into a framework for achieving the goal of a secure and resilient Nation. Resilience is the desired outcome, defined in the Goal as the "ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies."

Recipients will use the National Preparedness System to build, sustain, and deliver these core capabilities. The components of the National Preparedness System are Identifying and Assessing Risk; Estimating Capability Requirements; Building and Sustaining Capabilities; Planning to Deliver Capabilities; Validating Capabilities; and Reviewing and Updating. Additional details regarding the National Preparedness System and how it is supported by preparedness grant programs can be found in the program-specific chapters.

1.5. Strengthening Governance Integration

FEMA preparedness grant programs are intended to support the core capabilities across the five mission areas of Prevention, Protection, Mitigation, Response, and Recovery that are necessary to prepare for incidents posing the greatest risk to the Nation's security. Each program reflects the Department's intent to build and sustain an integrated network of national capabilities across all levels of government and the whole community.

Recipients must coordinate activities across preparedness disciplines and levels of government, including SLTT governments. A cohesive planning framework should incorporate FEMA resources, as well as those from other federal and SLTT entities, the private sector, and faith-based community organizations. Disparate governance structures, or processes for making decisions about how to spend grant funding, must be integrated and refined to ensure resources are targeted to support the most critical needs of a community based on risk-driven, capabilities-based planning. Strong governance systems ensure that disparate funding streams are coordinated and applied for maximum impact. Governance involving a broad range of stakeholders can effectively support a whole community approach to emergency preparedness and managing and enhancing core capabilities.

FEMA requires that all governance processes that guide the allocation of preparedness grant funds adhere to the following guiding principles:

- **Coordination of Investments**: Resources must be allocated to address the most critical capability needs and coordinated among affected preparedness stakeholders.

- **Transparency**: Stakeholders must be provided visibility on how preparedness grant funds are allocated and distributed, and for what purpose.
- **Substantive Local Involvement**: The tools and processes that are used to inform the critical priorities, which FEMA grants support, must include local government representatives. At the recipient level, local risk assessments must be included in the overarching analysis to ensure that all threats and hazards are accounted for.
- **Accountability**: FEMA recognizes that unique preparedness gaps exist at the local level. Grant recipients are responsible for ensuring the effective use of funds to address those gaps and for maintaining and sustaining existing capabilities.
- **Support of Regional Coordination**: Inter/intra-government entity partnerships and dependencies at the state, territorial, tribal, and regional levels, including those within metropolitan areas, must be recognized.

2. Award Determination and Obligation

2.1. Federal Award Administration Information

2.1.1. NOTICE OF AWARD

The Authorized Organization Representative (AOR) should carefully read the federal award package before accepting the federal award. The federal award package includes instructions on administering the federal award as well as terms and conditions for the award.

By submitting an application, applicants agree to comply with the prerequisites stated in the applicable NOFO, this manual, and the material terms and conditions of the federal award, should they receive an award.

FEMA will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent via the grant application system to the submitting AOR.

Recipients must accept their awards within **the time specified in the program-specific NOFO**. Recipients shall notify FEMA of their intent to accept the award and proceed with work via the FEMA GO system.

Funds will remain on hold until the recipient accepts the award via FEMA GO and all other conditions of the award have been satisfied, or until the award is otherwise rescinded. Failure to accept a grant award within the specified timeframe may result in a loss of funds.

For instructions on how to accept or decline an award in the FEMA GO system and for more information on FEMA GO generally, please see the FEMA GO page on FEMA.gov.

2.1.2. PASS-THROUGH REQUIREMENTS

Please see the applicable program-specific NOFO and chapter of this manual for information on pass-through requirements for that program.

3. Recipient and Subrecipient Costs

3.1. General Funding Requirements

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, the applicable NOFO, this manual, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period (which for FEMA preparedness grant awards is the same as the period of performance [POP]). See 2 C.F.R. § 200.403(h).

Recipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).

2. Lobbying and prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.

3. Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435).

In general, the 2 C.F.R. Part 200 Cost Principles establish standards for the allowability of costs, provide detailed guidance on the treatment of costs as direct or administrative costs, and set forth allowability principles for selected items of cost. More specifically, except as otherwise stated in the applicable program chapter to this manual, the program NOFO, or the terms and conditions of an award, costs charged to awards covered by this manual must be consistent with the Cost Principles for Federal Awards located at 2 C.F.R. Part 200, Subpart E. To be allowable, all costs charged to a FEMA award or applied to the cost share must be reasonable in nature and amount and allocable to the FEMA award.

If FEMA staff identify costs that are inconsistent with any of these requirements, these costs may be disallowed, and FEMA may recover funds as appropriate, consistent with applicable laws, regulations, and policies.

3.2. Direct Allowable Costs

Specific investments made in support of the funding priorities discussed in the NOFOs generally fall into one of the following eight allowable expense categories:

1. Construction;

2. Equipment;

3. Exercises;

4. Management & Administration (M&A);

5. Organization;

6. Operational Activities;

7. Planning; and

8. Training.

As this list is not exhaustive, refer to the relevant program-specific NOFO, this manual, and the program-specific point of contact for more information on allowable costs, funding restrictions, funding priorities, and these categories.

3.2.1. AUTHORIZED EQUIPMENT LIST

The Authorized Equipment List (AEL) is a list of approved equipment types allowed under FEMA's preparedness grant programs. The intended audience of this tool is emergency managers, first responders, and other homeland security professionals. The list consists of equipment categories divided into categories, sub-categories, and then individual equipment items. Contact your Preparedness Officer with questions on the AEL.

3.2.2. REQUIREMENTS FOR SMALL UNMANNED AIRCRAFT SYSTEMS

All grant-funded procurements of Small Unmanned Aircraft Systems (sUAS) must be executed in a manner compliant with federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327. For recipients that use grant funds for sUAS, FEMA advises that there is a general privacy concern related to the use of this equipment if the data the devices collect is transmitted to servers not under the control of the operator. Some manufacturers of sUAS may encrypt data and send that data to servers outside the United States. DHS's Privacy Office suggests the recipient fully explore data transmission and storage issues with vendors to reduce the possibility of data breaches.

Upcoming Prohibition on Covered Unmanned Aircraft Systems from Covered Foreign Entities

The American Security Drone Act of 2023, which was enacted as part of the National Defense Authorization Act for Fiscal Year 2024, Pub. L. No. 118-31 (41 U.S.C. § 3901 note prec. 3901), prohibits using federal award funds to procure or operate a covered unmanned aircraft system (UAS) from covered foreign entities. **This new prohibition will apply to all FEMA awards made on or after Dec. 22, 2025.**

A "covered unmanned aircraft system" under the American Security Drone Act of 2023 is an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (see 49 U.S.C. § 44801(12)).

The American Security Drone Act of 2023 requires publication on SAM.gov of a list of "covered foreign entities" developed and maintained by the Federal Acquisition Security Council. Please see SAM.gov for more information on the covered foreign entity list and monitor for any updates to the list as the prohibition date approaches.

Acquisition and Use of Technology to Mitigate Unmanned Aircraft Systems (Counter-Unmanned Aircraft System)

In August 2020, DHS, the Department of Justice (DOJ), the Federal Aviation Administration, and the Federal Communications Commission issued the Interagency Legal Advisory on Unmanned Aircraft Systems (UAS) Detection and Mitigation Technologies. The purpose of the advisory guidance

document is to help non-federal public and private entities better understand the federal laws and regulations that may apply to the use of capabilities to detect and mitigate threats posed by UAS operations (i.e., Counter-UAS or C-UAS).

The Departments and Agencies issuing the advisory guidance document, and FEMA, do not have the authority to approve non-federal public or private use of UAS detection or mitigation capabilities, nor do they conduct legal reviews of commercially available product compliance with those laws. The advisory does not address state and local laws nor potential civil liability, which UAS detection and mitigation capabilities may also implicate.

It is strongly recommended that, before the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation system and should not rely solely on vendors' representations of the systems' legality or functionality. Please also see the DHS press release on this topic for further information: Interagency Issues Advisory on Use of Technology to Detect and Mitigate Unmanned Aircraft Systems. For training on the application of UAS technology in emergency management programs, please refer to the National Preparedness Course Catalog and search 'UAS' on the website.

The Cybersecurity and Infrastructure Security Agency (CISA) offers several resources that detail the UAS threat environment and security protocols on the Unmanned Aircraft Systems Resources page on CISA.gov. Additional resources may be found on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) site.

Table 1: Unmanned Aircraft System Allowability

Grant Program	Allowed
HSGP (SHSP, UASI)	Yes
HSGP (OPSG)	Yes
THSGP	Yes
NSGP	No
TSGP	Yes
IPR Program	Yes
IBSGP	No
PSGP	Yes
EMPG Program	Yes

3.2.3. PROHIBITION ON COVERED EQUIPMENT OR SERVICES

Recipients, sub-recipients, and their contractors or subcontractors must comply with the prohibitions set forth in Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which restrict the purchase of covered telecommunications and surveillance equipment and

services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services for more information.

3.2.4. FUNDING FOR CRITICAL EMERGENCY SUPPLIES

Critical emergency supplies—such as shelf stable products, water, and basic medical supplies—are an allowable expense under the HSGP (SHSP and UASI only), THSGP, and EMPG Programs. Each state, urban area, or Tribal Nation must have FEMA's approval of a five-year viable inventory management plan prior to allocating grant funds for stockpiling purposes. The Inventory Management Plan should address how critical supplies will be maintained and sustained by the grant recipient and include a distribution strategy and related sustainment costs if the grant expenditure for these items is over $100,000. The Inventory Management Plan is associated with, but distinct from, the Distribution Management Plan, which addresses how supplies will be distributed in an emergency. For more information on distribution management planning, see FEMA's Distribution Management Plan Guide 2.0.

If grant expenditures exceed the minimum threshold, the five-year inventory management plan will be developed by the recipient and monitored by FEMA. FEMA will provide program oversight and technical assistance (TA) as it relates to the purchase of critical emergency supplies. FEMA will establish guidelines and requirements for the purchase of these supplies and monitor development and status of the recipient's inventory management plan.

Recipients are strongly encouraged to consult with their respective FEMA Regional Logistics Chief regarding disaster logistics-related issues. States are further encouraged to share their FEMA approved plan with local jurisdictions and Tribal Nations.

Table 2: Critical Emergency Supplies Allowability

Grant Program	Allowed
HSGP (SHSP, UASI)	Yes
HSGP (OPSG)	No
THSGP	Yes
NSGP	No
Surface Transportation Security Grants (TSGP, IBSGP, IPR Program)	No
PSGP	No
EMPG Program	Yes

3.3. Maintenance and Sustainment

The use of FEMA preparedness grant funds for maintenance contracts or agreements, warranty coverage, repair or replacement costs, licenses, upgrades, and user fees are allowable under all active and future grant awards, unless otherwise noted in the program-specific NOFO. Warranty and

sustainment coverage may exceed the POP if purchased as part of the original purchase of the system or equipment if the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts. When purchasing a stand-alone warranty or extending an existing maintenance contract on an already-owned piece of equipment system, coverage purchased may not exceed the POP of the award used to purchase the maintenance agreement or warranty. As with warranties and maintenance agreements, this extends to licenses and user fees, as well.

Preparedness grant funds are intended to support the Goal and fund activities and projects that build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats and hazards that pose the greatest risk to the security of the Nation. To assist recipients in meeting this objective, the expansion of eligible maintenance and sustainment costs must be:

1. In direct support of existing capabilities;

2. An otherwise allowable expenditure under the applicable grant program;

3. Tied to one of the core capabilities in the five mission areas contained within the Goal; and

4. **For the HSGP (SHSP and UASI) and EMPG Program only**, shareable through the Emergency Management Assistance Compact (EMAC).

Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant funding or any other source of funding other than FEMA preparedness grant program dollars.

For the HSGP, stand-alone warranties can only cover equipment purchased with HSGP funds or for equipment dedicated for HSGP-related purposes.

For the PSGP, maintenance and sustainment are focused specifically on the repair and replacement of existing equipment and does not include routine activities such as oil changes or washing/cleaning existing equipment.

For more information on maintenance and sustainment costs, see the program-specific chapter below and/or the applicable NOFO.

3.4. Management and Administration

Management and administration (M&A) costs are for activities directly related to the management and administration of the award, such as financial management, reporting, and program and financial monitoring. M&A costs are not operational costs, they are the necessary costs incurred in direct support of the grant or as a result of the grant and should be allocated across the entire lifecycle of the grant. Characteristics of M&A expenses can include the following: 1) direct costs that are incurred to administer a particular federal award; 2) identifiable and unique to each federal award; 3) charged based on the activity performed for that federal award; and 4) not duplicative of the same costs that are included in the approved Indirect Cost Rate Agreement, if applicable.

Some examples of M&A costs include grants management training for M&A staff, equipment and supplies for M&A staff to administer the grant award, travel costs for M&A staff to attend conferences or training related to the grant program, travel costs for the M&A staff to conduct subrecipient monitoring, contractual services to support the M&A staff with M&A activities, and

auditing costs related to the grant award to the extent required or permitted by statute or 2 C.F.R. Part 200. For additional program-specific M&A information, please refer to the relevant program-specific NOFO.

3.5. Procedures for Establishing Indirect Cost Rates

Indirect costs (per 2 C.F.R. § 200.1) are incurred for a common or joint purpose benefitting more than one cost objective, and not readily assignable to the cost objectives specifically benefitted, without effort disproportionate to the results achieved. Indirect costs are allowable under all programs covered by this manual. The requirements and procedures for establishing indirect cost rates are the same for all the preparedness programs covered by this manual. The process for establishing the indirect cost rate (per 2 C.F.R. § 200.414) varies based on the type of entity and the amount of funding they receive:

- If the entity is a non-governmental entity (e.g., institutions of higher education/hospital, nonprofit organization, etc.), and is a subrecipient, indirect cost rate procedures are outlined in 2 C.F.R. § 200.332(a)(4) and Appendices III, IV, IX to Part 200. These types of entities may either use the de minimis rate or negotiate a rate with the pass-through entity.

- If the subrecipient is a state or local governmental entity, indirect cost rate procedures are established in Appendix VII to Part 200.

    - Per Paragraph D.1.b. of Appendix VII, state or local governmental entities receiving grant funds must develop an indirect cost rate proposal.

        - If the state or local entity receives more than $35 million in grant funding in a fiscal year, the proposal must be approved by the cognizant agency.

        - If a state or local entity receives $35 million or less in grant funding in a fiscal year, they must develop an indirect cost rate proposal, but that indirect cost rate proposal does *not* need to be approved by the cognizant agency.

- The de minimis rate does not require documentation to justify its use and may be used indefinitely (per 2 C.F.R. § 200.414(f)).

4. Administrative and National Policy Requirements

A recipient under the programs covered by this manual must comply with the DHS Standard Terms and Conditions in effect as of the date of the federal award. The DHS Standard Terms and Conditions are available online: DHS Standard Terms and Conditions. For continuation awards, the terms and conditions for the initial federal award will apply unless otherwise specified in the terms and conditions of the continuation award. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

4.1. Presidential Executive Orders

Recipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

In accordance with Executive Order 14305, Restoring American Airspace Sovereignty (June 6, 2025), and to the extent allowed by law, eligible state, local, tribal, and territorial grant recipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state, local, tribal, and territorial agencies. Recipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

4.2. Subrecipient Monitoring and Management

Pass-through entities must comply with the requirements for subrecipient monitoring and management as set forth in 2 C.F.R. §§ 200.331-333.

4.3. Accessibility Compliance

Preparedness grant program recipients using funds to build or alter buildings must comply with the applicable accessibility requirements under their local building codes, as well as the Section 504 Rehabilitation Act of 1973, 29 U.S.C. § 794, the Architectural Barriers Act of 1968 (ABA), and the Americans with Disabilities Act (ADA), 42 U.S.C. §§ 12101 et seq., to ensure individuals with disabilities have access to such buildings. State and local governments are required to provide qualified individuals with disabilities equal access to their programs, services, or activities, unless doing so would fundamentally alter the nature of their programs, services or activities or would impose an undue burden. Accessibility standards under the ABA and ADA are highly similar. Additional information regarding compliance with the ABA is available at Chapter 1: Using the ABA Standards on access-board.gov.

4.4. Adaptive Support

Pursuant to Section 504 of the Rehabilitation Act of 1973, recipients of FEMA financial assistance must ensure that their programs and activities do not discriminate against qualified individuals with disabilities.

4.5. Environmental Planning and Historic Preservation Compliance

FEMA is required to consider effects of its actions on the environment and historic properties to ensure that activities, grants and programs funded by FEMA, comply with federal Environmental Planning and Historic Preservation (EHP) laws, Executive Orders, regulations, and policies.

Recipients and subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures, and facilities, and/or new construction and/or replacement of buildings, structures, and facilities, must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species, historic properties, or communities with environmental concerns; submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and, identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen impacts to EHP resources and bring the project into EHP compliance.

EHP guidance is found at Environmental Planning and Historic Preservation. The site contains links to documents identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also found in the EHP Directive & Instruction.

All FEMA actions, including grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or building code (44 C.F.R. § 9.11(d)(6)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions, including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features and nature-based solutions may be incorporated into actions as minimization measures.

The GPD EHP screening form is located on FEMA's website. The form should be submitted to gpdehpinfo@fema.dhs.gov and your assigned Preparedness Officer.

4.5.1. CONSTRUCTION AND RENOVATION

All construction and renovation projects require EHP review. Recipients and subrecipients are encouraged to have completed as many steps as possible for a successful EHP review in support of their proposal for funding (e.g., coordination with their State Historic Preservation Office to identify potential historic preservation issues and to discuss the potential for project effects, compliance with all state and local EHP laws and requirements). Projects for which the recipient believes an Environmental Assessment (EA) may be needed, as defined in DHS Instruction Manual 023-01-001-01, Revision 01, FEMA Directive 108-1, and FEMA Instruction 108-1-1, must also be identified to the FEMA HQ Preparedness Officer within 6 months of the award and completed EHP review materials must be submitted no later than 12 months before the end of the POP. EHP policy guidance and the

EHP Screening Form can both be found on FEMA.gov. EHP review materials should be sent to gpdehpinfo@fema.dhs.gov.

Refer to the program-specific NOFO for information on construction and renovation allowability and restrictions.

4.5.2. COMMUNICATION TOWERS

For the purposes of the limitations on funding levels only, communication towers are not considered construction. When applying for construction funds, including communications towers, recipients must submit evidence of approved zoning ordinances, architectural plans, and any other locally required planning permits at the time of application.

All construction of communication towers requires EHP review. When applying for funds to construct communication towers, recipients and subrecipients must submit evidence that the Federal Communication Commission's Section 106 of the National Historic Preservation Act, Pub. L. No. 89-665, as amended, review process has been completed and submit all documentation resulting from that review to FEMA with an EHP Screening Form and supporting materials for EHP review. Recipients and subrecipients are encouraged to have completed as many steps as possible for a successful EHP review in support of their proposal for funding (e.g., coordination with their state, tribal, or territorial Historic Preservation Office to identify potential historic preservation issues and to discuss the potential for project effects, compliance with all state and local EHP laws and requirements). Projects for which an EA may be needed, as defined in DHS Instruction Manual 023-01-001-01, Revision 01, FEMA Directive 108-1, and FEMA Instruction 108-1-1, must also be identified to the FEMA HQ Preparedness Officer within 6 months of the award. Completed EHP review materials must be submitted no later than 12 months before the end of the POP. EHP policy guidance and the EHP Screening Form can both be found on FEMA.gov. EHP review materials should be sent to gpdehpinfo@fema.dhs.gov.

4.5.3. HAZARD RESISTANT BUILDING CODES

Hazard-resistant building codes are a foundational element of a more resilient nation, safeguarding communities and lives against natural disasters, with an estimated $11:1 return on investment. The adoption, enforcement and application of modern building codes mitigates community vulnerabilities, reduces disaster recovery costs, and strengthens nationwide capability. FEMA is working to promote and support building codes in all areas of its work in support of the multi-agency National Initiative to Advance Building Codes. In the interest of building a stronger, more resilient nation, FEMA encourages all grant recipients and subrecipients to meet current published editions of relevant consensus-based building codes, specifications and standards, and to exceed them where feasible.

4.6. Domestic Preferences for Procurement

The recipient or subrecipient should, to the greatest extent practicable and consistent with law, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States. This includes, but is not limited to, iron, aluminum, steel, cement, and other manufactured products.

4.6.1. CONTRACT PROVISION REQUIREMENT

All FEMA recipients and subrecipients are required to include in all contracts and purchase orders for work or products a contract provision encouraging domestic preference for procurements. Programs receiving federal financial assistance for infrastructure projects may also be subject to the Build America, Buy America Act preferences set forth in 2 C.F.R. Part 184. See Section 7.7 for more information.

Sample Contract Clause

> *"Domestic Preference for Procurements. The Contractor should, to the greatest extent practicable and consistent with law, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States. This includes, but is not limited to, iron, aluminum, steel, cement, and other manufactured products. For purposes of this clause: Produced in the United States means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States."*

4.7. Financial Assistance Programs for Infrastructure

Recipients and subrecipients must comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA). See 2 C.F.R. Part 184, Buy America Preferences for Infrastructure Projects and Office of Management and Budget (OMB), Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

None of the funds provided under the grants covered by this manual may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States. Additional information on the Buy America preference can be found in the program-specific NOFO and at the "Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure page on FEMA's website.

4.8. Davis-Bacon Act Compliance

Recipients using funds for construction projects must comply with the Davis-Bacon Act (codified as amended at 40 U.S.C. §§ 3141 *et seq*.). *See* 6 U.S.C. § 609(b)(4)(B) (cross-referencing 42 U.S.C. §5196(j)(9), which cross-references Davis-Bacon). Recipients must ensure that their contractors or subcontractors for construction projects pay workers no less than the prevailing wages for laborers and mechanics employed on projects of a character similar to the contract work in the civil subdivision of the state in which the work is to be performed. Additional information regarding compliance with the Davis-Bacon Act, including Department of Labor (DOL) wage determinations, is available from the Davis-Bacon and Related Acts page on DOL.gov.

4.9. National Incident Management System Implementation

National Incident Management System (NIMS) guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System. As recipients and subrecipients of federal preparedness (ND) grant awards, jurisdictions and organizations must achieve, or be actively working to achieve, all the

NIMS Implementation Objectives. These objectives and implementation information can be found on the NIMS and NIMS Implementation and Training pages on FEMA.gov.

Emergency management and incident response activities require carefully managed resources (personnel, teams, facilities, equipment, and/or supplies) to meet incident needs. NIMS defines a national, interoperable approach for sharing resources, coordinating, and managing incidents, and communicating information. Incident management refers to how incidents are managed across all homeland security activities, including prevention, protection, mitigation, response, and recovery. Utilization of the standardized resource management concepts such as typing, credentialing, and inventorying promote a strong national mutual aid capability needed to support the delivery of core capabilities. Additional information on resource management, NIMS resource typing definitions, job titles, and position qualifications is available at the NIMS Components – Guidance and Tools page on FEMA.gov. Please also see the relevant NOFOs for additional requirements regarding NIMS implementation for specific programs.

4.9.1. NIMS GUIDANCE FOR THE NATIONAL QUALIFICATION SYSTEM

FEMA developed the NIMS Guideline for the National Qualification System (NQS) to describe national credentialing standards and to provide written guidance regarding the use of those standards. This guideline describes credentialing and typing processes and identifies tools that Federal Emergency Response Officials and emergency managers at all levels of government may use both routinely and to facilitate multijurisdictional coordinated responses. **Starting in FY 2023, EMPG Program recipients are required to use EMPG Program funds to support NQS implementation efforts.**

The NQS doctrine promotes interoperability by establishing a common language for defining job titles and by enabling jurisdictions and organizations to plan for, request, and have confidence in the capabilities of personnel deployed for disasters and emergencies from other entities through mutual aid agreements and compacts. Following the concepts and processes in this Guideline will enhance national preparedness by expanding the network of qualified incident management and support personnel who can be deployed nationwide.

4.10. SAFECOM Guidance Compliance

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

Departments and agencies at all levels of government have identified a need for improvement in several high-priority areas, including Governance, Planning, Training and Exercises, Operational Coordination, and Technology. In addition, communications resilience and continuity should be viewed as a critical component within each of these areas. These priorities are explained in detail in Section 2 of the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). By addressing these priorities, which are reflective of proven best practices, emergency communications can be significantly improved at all levels of government. The end goal is to ensure

operable, interoperable, and resilient communications that maintain a continuous flow of critical information, under all conditions, among multi-jurisdictional and multi-disciplinary emergency responders, command posts, agencies, critical infrastructure sectors, and government officials for the duration of an emergency response operation, and in accordance with NIMS and the National Emergency Communications Plan (NECP), which describes goals and objectives for improving emergency communications nationwide.

To help meet this goal, the SAFECOM Guidance outlines requirements for grant applications, including alignment to national, regional, and state communications plans (e.g., NECP, Statewide Communication Interoperability Plan (SCIP), Tactical Interoperability Communications Plan (TICP), FEMA Regional Emergency Communications Plan (RECP)), project coordination, and technical standards for emergency communications technologies (e.g., Project 25 (P25) standards for land mobile radio equipment). SCIPs define the current and future direction for interoperable and emergency communications within a state or territory, while TICPs are designed to allow urban areas, counties, regions, states/territories, Tribal Nations, or federal departments/agencies to document interoperable communications governance structures, technology assets, and usage policies and procedures. In addition, FEMA's formal planning process has produced 10 RECPs and their associated state and/or tribal/territorial annexes that identify emergency communications capability shortfalls and potential resource requirements. Grant recipients are encouraged to leverage these planning resources as a source of input and reference for all emergency communications grant applications and investment justifications (IJ).

In addition, FEMA formally recognizes several statewide emergency communications governance bodies (e.g., Statewide Interoperability Coordinator (SWIC), Statewide Interoperability Governance Board (SIGB), Statewide Interoperability Executive Committee (SIEC), FirstNet State Single Point of Contact (SPOC)), and strongly encourages grant recipients to closely coordinate with these entities when developing an emergency communications investment to ensure projects support the state or territory's strategy to improve their communications capabilities with the goal of achieving fully operable, interoperable, and resilient communications. In addition, recipients should work with public and private entities, and across jurisdictions and disciplines, to demonstrate engagement with the whole community in accordance with Presidential Policy Directive-8 (PPD-8).

For regional, cross-border initiatives, FEMA requires recipients to coordinate projects with national level emergency communications coordination bodies, such as the National Council of Statewide Interoperability Coordinators (NCSWIC) and the Regional Emergency Communications Coordination Working Groups (RECCWG). NCSWIC promotes and coordinates state-level activities designed to ensure the highest level of public safety communications across the nation. RECCWGs are congressionally mandated planning and coordination bodies located in each FEMA Region and provide a collaborative forum to assess and address the survivability, sustainability, operability, and interoperability of emergency communications systems at all levels of government (6 U.S.C. § 575). Grant-funded investments that are coordinated with these bodies will help ensure that federally funded emergency communications investments are interoperable and support national policies.

All entities using preparedness grant funding to support emergency communications investments are required to comply with the SAFECOM Guidance. The SAFECOM Guidance provides current information on emergency communications policies, eligible costs, best practices, and technical standards for SLTT recipients investing federal funds in emergency communications projects. It is also designed to promote and align with the NECP. Compliance with the SAFECOM Guidance helps ensure that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. Applicants should use the SAFECOM Guidance during planning, development, and implementation of emergency communications projects and in conjunction with other planning documents (e.g., SCIPs).

Specifically, Appendix D of the SAFECOM Guidance contains compliance instructions for FEMA grant recipients.

Emergency communications investments also will be reviewed jointly by FEMA and CISA to verify compliance with SAFECOM Guidance. FEMA will coordinate directly with the recipient on any compliance concerns and will provide TA as necessary to help ensure full compliance. Please see the program-specific NOFOs for more information and instructions regarding SAFECOM compliance.

4.11. Resilient Communications Guidance

The risk imposed by the reliance on communication systems by government and the private sector can be reduced by understanding dependencies, analyzing effects, and taking action. Entities planning to use preparedness grant funding for communications investments are encouraged to take a whole community approach and work with state emergency management agencies, SWICs, SIGBs, and appropriate stakeholders at the regional and SLTT levels to:

- Plan communication around the whole community to meet everyone's needs.
- Establish robust, resilient, reliable, and interoperable communications capabilities. Account for the mission impact of communication system disruptions in your planning;
- Ensure mission-related communications (voice, video, data, and network security requirements) are adequately planned for and understood. It is important to maintain current documentation of your communication systems architecture and perform regular audits. Your ability to continue operations is dependent on the availability of and access to communications systems with sufficient resiliency, redundancy, and accessibility to perform essential functions and provide critical services during a disruption;
- Ensure critical communication systems connectivity among key government leadership, internal elements, other supporting organizations, and the public under all conditions. As such, organizations should ensure current copies of vital records, including electronic files and software, are backed-up and maintained off-site;
- Ensure all communications systems/networks are traced from end to end to identify all Single Points of Failure (SPF). In doing so, recipients should work with communication service providers to add redundancy at key critical infrastructure facilities as needed;
- Ensure key communication systems resiliency through:
    - Ensuring availability of backup systems;
    - Ensuring diversity of network element components and routing;
    - Ensuring geographic separation of primary and alternate transmission media;
    - Ensuring availability of back-up power sources;
    - Ensuring availability and access to systems that are not dependent on commercial infrastructure;
    - Maintaining spares for designated critical communication systems; and

  - Working with commercial suppliers to remediate communication SPF.

- All communications system owners are encouraged to address the following issues:
  - Integrate communications needs into continuity planning efforts by incorporating Primary, Alternate, Contingency, and Emergency (PACE) methodology, and vulnerability mitigation options to ensure uninterrupted communications support;
  - Establish a cybersecurity plan that includes continuity of a communications component such as Radio Frequency (RF)-based communications that do not rely on public infrastructure;
  - Maintain communications capabilities to ensure their readiness when needed;
  - Frequently train and exercise personnel required to operate communications capabilities;
  - Test and exercise communications capabilities; and
  - Consider Electromagnetic Pulse (EMP) protective measures for communications systems and emergency backup power where practical.

CISA Emergency Communication Division enhances public safety interoperable communications at all levels of government and conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to communicate in the event of natural disasters, acts of terrorism, and other hazards. CISA provides plans, resources, and training to support operable and interoperable emergency communications for first responders. For additional information visit CISA's Emergency Communications page.

4.12. FirstNet

The Middle-Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, as amended (codified in part at 47 U.S.C. §§ 1401-1473) established the First Responder Network Authority (hereinafter FirstNet Authority) as an independent authority within the National Telecommunications and Information Administration (NTIA). 47 U.S.C. § 1424(a). The FirstNet Authority's statutory mission is to establish a nationwide public safety broadband network (FirstNet). 47 U.S.C. § 1426(b). FirstNet uses the 700 MHz D block spectrum to provide Long-Term Evolution (LTE)-based broadband services and applications to public safety entities. 47 U.S.C. §§ 1401(2), 1421(a). FirstNet became operational in March 2018 and is based on a single, national network architecture that evolves with technological advances and consists of a physically separate evolved packet core (EPC) network and radio access networks (RANs).

FirstNet provides public safety entities with mission-critical broadband data capabilities and services including, but not limited to messaging, image sharing, video streaming, group text, voice, data storage, application, location-based services, and Quality of Service, Priority, and Preemption. Public safety entities seeking to enhance their operational capabilities using broadband technology may seek grant funding from appropriate programs to support the following:

- Planning for integration of information technology (IT) infrastructure, software, and site upgrades necessary to connect to FirstNet;
- Handheld broadband devices including smartphones, feature phones, tablets, wearables, push-to-talk (PTT) devices;

- Vehicle-mounted or otherwise field operated data devices, such as ruggedized laptops;
- Network access devices, including portable Wi-Fi devices, Universal Serial Bus (USB) modems/dongles, trunk-mounted modems, routers;
- Customer-Owned and Managed (COAM) broadband deployable equipment, enabling public safety to own and dispatch coverage expansion or capacity enhancement equipment within their jurisdiction;
- Broadband device accessories that enable efficient and safe public safety operations such as headsets, belt clips, earpieces, remote Bluetooth sensors, ruggedized cases;
- Subscriber Identification Modules (SIMs)/Universal Integrated Circuit Cards (UICCs) to allow public safety users to update existing devices to operate on public safety prioritized services; and
- One-time purchase and subscription-based applications for public safety use which could include, among several other options, enterprise mobility management (EMM), mobile device management (MDM), mobile Virtual Private Network (VPN), identity services, or cloud service tools.

As FirstNet is built out in all 56 states and territories, and coverage and capacity for first responders expands, recipients are strongly encouraged to coordinate with SWIC and FirstNet on the planning, deployment timelines, and operational availability of the network deployment within a specific state or territory, and to ensure that the project does not conflict with network planning efforts and complies with all technical requirements. FirstNet requires participating agencies to demonstrate a subscription to public safety-prioritized broadband services to purchase FirstNet broadband devices or applications. Recipients must coordinate with FirstNet in advance of any strategic acquisition of broadband LTE equipment to ensure that purchases adhere to all applicable standards for public safety entities. Recipients with questions on FirstNet should contact info@firstnet.gov. Please also refer to the most recent SAFECOM Guidance for additional guidance.

4.13. Department of Homeland Security/FEMA Communications Support Services

CISA and FEMA offer a variety of TA and other support services to assist state and local entities in their efforts to comply with the above requirements, including the SAFECOM Guidance, with the goal of ensuring interoperable and resilient emergency communications. A summary of DHS support services is provided below. Grant recipients are encouraged to refer to the respective websites for additional information.

4.13.1. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY SUPPORT

CISA assists agencies through a myriad of services, including direct TA and training provided at no cost to the jurisdiction. The TA offerings include (but are not limited to):

- Coordinated statewide governance (e.g., State Mapping Tool, Interoperable Communications Reference Guides);
- Comprehensive emergency communications planning (e.g., SCIPs, TICPs, and Field Operations Guides);

- Next Generation 911 planning and implementation;
- Data operability and interoperability;
- Alerts and warnings;
- Broadband deployment;
- Cybersecurity education and awareness; and
- Communications Unit (COMU) planning and procedures.

Information on these services is available at the CISA Interoperable Communications Technical Assistance Program (ICTAP) Resources page on CISA.gov.

4.13.2. FEMA DISASTER EMERGENCY COMMUNICATIONS DIVISION SUPPORT

FEMA Disaster Emergency Communications (DEC) deploys, installs, operates, maintains, and protects telecommunications, logistics, and operations assets in support of planned special events and in response to disasters, assisting citizens and first responders.

DEC provides DEC through six geographically dispersed Mobile Emergency Response Support (MERS) detachments and a pre-positioned fleet of Mobile Communications Office Vehicles (MCOV). DEC also assists SLTT entities in mitigating their DEC risks and requirements to support life-saving efforts, protect property, and coordinate response and recovery operations. DEC can assist SLTT entities in mitigating their DEC risks and requirements to support life-saving efforts, protect property, and coordinate response and recovery operations. For more information about how DEC can provide stakeholder support in these areas, see the DEC page on FEMA.gov.

4.13.3. FEMA NATIONAL PREPAREDNESS DIRECTORATE SUPPORT

National Preparedness Directorate (NPD) provides training, exercises, and TA to SLTT stakeholders that support operational and emergency communications. Descriptions and resources specific to operational communication are available on FEMA.gov's Core Capability Development Sheets page within the Response Mission Area and include the following information to support jurisdictions:

- Description of the operational communications core capability;
- Training for building and sustaining operational communication with specific course titles:
    - Trainings can also be found at National Training and Education Division (NTED) page on firstrespondertraining.gov.
- Example capability targets to complete a Threat and Hazard Identification and Risk Assessment (THIRA):
    - Help in developing targets can be found at Unified Reporting Tool (URT)-Info page on FEMA's Preparedness Toolkit or requested at FEMA-SPR@fema.dhs.gov.
- Tools to validate capabilities through exercises:

- TA and support from subject-matter experts can be requested through the Exercises page on FEMA.gov.

4.13.4. FEMA OFFICE OF NATIONAL CONTINUITY PROGRAMS SUPPORT

The Office of National Continuity Program's (ONCP) support services focus on holistic continuity planning, of which communications continuity is an important component. Currently, continuity communications training and TA is limited to the FEMA National Radio System (FNARS), Integrated Gateway System (IGS), the Continuity Communications Satellite System, and the Integrated Public Alerts & Warning System (IPAWS) and is delivered either through scheduled webinars or on an ad hoc basis at the request of the state entity, through a FEMA Region, or via a requirement for terms of use.

5. Post-Award Management and Implementation

5.1. Reporting

Recipients are required to submit various financial and programmatic reports as a condition of award acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

Consultants or contractors are not permitted to be the AOR or the Signatory Authority (SA) of the recipient. The AOR, as the Authorized Official for the award, is responsible for submitting programmatic and financial performance reports, accepting award packages, signing assurances and certifications, and submitting award amendments.

5.2. Federal Financial Reporting Requirements

5.2.1. FEDERAL FINANCIAL REPORT

1. Recipients must report obligations and expenditures through a federal financial report. The Federal Financial Report (FFR) form, also known as Standard Form 425 (SF-425), is available online at: SF-425 OMB #4040-0014.

2. Recipients must submit the FFR quarterly throughout the period of performance (POP) as detailed below in the following section.

3. The final FFR is due within 120 calendar days after the end of the POP.

FEMA may withhold future federal awards and cash payments if the recipient does not submit timely financial reports or the financial reports submitted demonstrate lack of progress or provide insufficient detail.

Recipients must file the FFR electronically using FEMA GO. Note that recipients for awards covered in this manual made before FY 2024 must file the FFR using the Payment and Reporting Systems (PARS).

Financial Reporting Periods and Due Dates

An FFR must be submitted quarterly throughout the POP, including partial calendar quarters, as well as in periods where no grant award activity occurs. The final FFR is due within 120 days after the end of the POP. Future awards and fund drawdowns may be withheld if these reports are delinquent, demonstrate a lack of progress, or are insufficient in detail.

Table 3 shows the reporting periods and due dates for the FFR, except for the final FFR due at 120 days after the end of the POP for purposes of closeout.

Table 3: FFR Reporting Periods and Due Dates

FFR Reporting Period	Report Due Date
Oct. 1–Dec. 31	Jan. 30

FFR Reporting Period	Report Due Date
Jan. 1–March 31	April 30
April 1–June 30	July 30
July 1–Sept. 30	Oct. 30

Because of a system limitation, if at the end of the POP for awards made before FY 2023a recipient still has funds to draw down, PARS requires an FFR be submitted within 30 days of the end of the POP to access those funds. In that case, the recipient will need to submit an FFR within 30 days of the end of the POP in addition to the final FFR within 120 days of the end of the POP. All other recipients who do not need to draw down funds after the end of the POP are only required to submit the final FFR within 120 days after the end of the POP.

5.3. Program Performance Reporting Requirements

5.3.1. PERFORMANCE PROGRESS REPORTS

Recipients are responsible for providing performance reports to FEMA on a biannual (twice a year) or quarterly (four times a year) basis via FEMA GO. The Performance Progress Reports (PPR) should include the following:

- A brief narrative of overall project(s) status;
- A summary of project expenditures; and
- A description of any potential issues that may affect project completion.

For the **EMPG Program only**, recipients are responsible for providing performance reports to FEMA on a quarterly (four times a year) basis via FEMA GO. As explained in Section 12.10.1 "Standardized Programmatic Reporting for the EMPG Program," the quarterly PPRs must use or be based on the approved EMPG Program Work Plan template provided in the EMPG Program NOFO.

Program Performance Reporting Periods and Due Dates

The biannual PPRs are due no later than 30 days after the end of the reporting period. Table 4 shows the reporting periods and due dates for biannual PPRs.

Table 4: Biannual PPR Reporting Periods and Due Dates

Reporting Period	Report Due Date
Jan. 1 – June 30	July 30
July 1 – Dec. 31	Jan. 30

Program Performance Reporting Periods and Due Dates for the Emergency Management Performance Grant Program

The quarterly PPRs are due no later than 30 days after the end of the quarter. Table 5 shows the reporting periods and due dates for the quarterly PPRs for the EMPG Program only.

Table 5: Quarterly PPR Reporting Periods and Due Dates (EMPG Program)

Reporting Period	Report Due Date
Oct. 1 – Dec. 31	Jan. 30
Jan. 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – Sept. 30	Oct. 30

5.4. Biannual Strategy Implementation Report

Applicable to the HSGP, THSGP, NSGP, and EMPG Program only.

In addition to the financial and performance progress reports, recipients are responsible for completing and submitting the Biannual Strategy Implementation Report (BSIR) through the FEMA GO system. For all HSGP, THSGP, NSGP, and EMPG Program awards made before FY 2024, the BSIR was completed in the Grants Reporting Tool.

The BSIR is due within 30 days after the end of the reporting period: July 30 for the reporting period of Jan. 1 through June 30 (summer BSIR report); and Jan. 30for the reporting period of July 1 through December 31 (winter BSIR report). All required attributes of each project must be included. Updated obligations, expenditures, and significant developments must be provided within the BSIR to show the progress of implementation for every project as well as how expenditures support Planning, Organization, Equipment, Training, and Exercises. The first BSIR for a given fiscal year award will be due by Jan. 30, or 30 days after the end of the first reporting period of the award. Subsequent BSIR reports will require recipients to report on a project-by-project basis.

Recipients also are responsible for completing and submitting a closeout BSIR. When an award's POP or the liquidation period ends in the middle of a reporting period, a traditional or "regular" BSIR must be submitted with full accounting of actual project information/expenditures before a Closeout BSIR can be created and submitted. Once FEMA approves the last "regular" BSIR, the Closeout BSIR can be created and submitted. Please contact your respective FEMA Preparedness Officer for questions regarding the BSIR.

5.5. Closeout Reporting Requirements

Within **120 days** after the end of the POP, or after an amendment has been issued to close out a federal award, recipients must submit the following in FEMA GO:

1. The final request for payment, if applicable.

2. The final FFR.

3. The final PPR detailing all accomplishments.

4. A qualitative narrative summary of the impact of those accomplishments throughout the POP.

5. Other documents required by the NOFOs, terms and conditions of the federal award, or other DHS Component guidance. This includes the program-specific chapters of this manual and other FEMA guidance.

After FEMA approves these reports, it will issue a closeout notice. The notice will indicate the POP as closed, list any remaining funds to be de-obligated, and address the record maintenance requirement. Unless a longer period applies, such as due to an audit or litigation, for equipment or real property used beyond the POP, or due to other circumstances outlined in 2 C.F.R. § 200.334, this maintenance requirement is three years from the date of the final FFR.

Also, pass-through entities are responsible for closing out those subawards as described in 2 C.F.R. § 200.344; subrecipients are still required to submit closeout materials within **90 calendar days** of the subaward POP end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions in time for the recipient to submit all necessary documentation and information to FEMA during the closeout of their prime award. The recipient is responsible for returning any balances of unobligated or unliquidated funds that have been drawn down that are not authorized to be retained per 2 C.F.R. § 200.344(e).

5.6. Administrative Closeout

Administrative closeout is a mechanism for FEMA to unilaterally execute closeout of an award. FEMA will use available award information in lieu of final recipient reports, per 2 C.F.R. § 200.344(h)-(i). It is an activity of last resort, and if FEMA administratively closes an award, this may negatively impact a recipient's ability to obtain future funding.

5.7. Disclosing Information per 2 C.F.R. § 180.335

Before entering into a federal award, the applicant must notify FEMA if it knows that the applicant or any of the principals (as defined at 2 C.F.R. § 180.995) for the federal award:

1. Are presently excluded or disqualified;

2. Have been convicted within the preceding three years of any of the offenses listed in § 180.800(a) or had a civil judgment rendered against you for one of those offenses within that time period;

3. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with the commission of any of the offenses listed in § 180.800(a); or

4. Have had one or more public transactions (Federal, State, or local) terminated within the preceding three years for cause or default.

This is requirement is fully described in 2 C.F.R. §180.335.

Additionally, 2 C.F.R. § 180.350 requires recipients to provide immediate notice to FEMA at any time after entering a federal award if:

1. The recipient learns that either it failed to earlier disclose information as required by 2 C.F.R. § 180.335;

2. Due to changed circumstances, the applicant or any of the principals for the federal award now meet the criteria at 2 C.F.R. § 180.335 listed above.

5.8. Reporting of Matters Related to Recipient Integrity and Performance

Appendix XII to 2 C.F.R. Part 200 states the terms and conditions for recipient integrity and performance matters used for this funding opportunity.

If the total value of all active federal grants, cooperative agreements, and procurement contracts for a recipient exceeds $10,000,000 at any time during the POP:

1. The recipient must maintain the currency of information reported in SAM.gov about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII;

2. The required reporting frequency is described in paragraph 4 of Appendix XII.

6. Additional Information

6.1. Monitoring and Oversight

6.1.1. OVERVIEW

Per 2 C.F.R. § 200.337, FEMA, through its authorized representatives, has the right, at all reasonable times, to make site visits or conduct desk reviews to review project accomplishments and management control systems to evaluate award progress and to provide any required TA. During site visits or desk reviews, FEMA will review recipients' files related to the award. As part of any monitoring and program evaluation activities, recipients must permit FEMA, upon reasonable notice, to review grant-related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a timely and accurate manner to FEMA requests for information relating to the award.

Effective monitoring and oversight help FEMA ensure that recipients use grant funds for their intended purpose(s), verify that projects undertaken are consistent with approved plans, and ensure that recipients make adequate progress toward stated goals and objectives. Additionally, monitoring serves as the primary mechanism to ensure that recipients comply with applicable laws, rules, regulations, program guidance, and requirements. FEMA regularly monitors all grant programs both financially and programmatically in accordance with federal laws, regulations (including 2 C.F.R. Part 200), program guidance, and the terms and conditions of the award. All monitoring efforts ultimately serve to evaluate progress toward grant goals and proactively target and address issues that may threaten grant success during the POP.

FEMA staff will periodically monitor recipients to ensure that administrative processes, policies and procedures, budgets, and other related award criteria are meeting federal government-wide and FEMA regulations. Aside from reviewing quarterly financial and programmatic reports, FEMA may also conduct enhanced monitoring through desk-based reviews, onsite monitoring visits, or both. Enhanced monitoring will involve the review and analysis of financial compliance and administrative processes, policies, activities, and other attributes of each federal assistance award, and it will identify areas where the recipient may need TA, corrective actions, or other support.

Financial and programmatic monitoring are complementary processes within FEMA's overarching monitoring strategy that function together to ensure effective grants management, accountability, and transparency; validate progress against grant and program goals; and safeguard federal funds against fraud, waste, and abuse. Financial monitoring primarily focuses on statutory and regulatory compliance with administrative grant requirements, while programmatic monitoring seeks to validate and assist in grant progress, targeting issues that may be hindering project goals and ensuring compliance with the purpose of the grant and grant program. Both monitoring processes are similar in that they feature initial reviews of all open awards and in-depth monitoring of grants requiring additional attention.

Recipients and subrecipients who are pass-through entities are responsible for monitoring their subrecipients in a manner consistent with the terms of the federal award at 2 C.F.R. Part 200, including 2 C.F.R. § 200.332. This includes the pass-through entity's responsibility to monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward, and that subaward performance goals are achieved.

In terms of overall award management, recipient and subrecipient responsibilities include—but are not limited to—accounting of receipts and expenditures, cash management, maintaining adequate financial records, reporting, and refunding expenditures disallowed by audits, monitoring if acting as a pass-through entity, other assessments and reviews, and ensuring overall compliance with the terms and conditions of the award or subaward, as applicable, including the terms of 2 C.F.R. Part 200. Similar civil rights monitoring and oversight may be conducted pursuant to 44 C.F.R. Part 7.

6.1.2. FINANCIAL MONITORING OVERVIEW AND APPROACH

FEMA's approach to financial monitoring provides a standard monitoring framework that promotes consistent processes across all monitoring staff. There are four core components of the monitoring process:

1. **Monitoring Assessment:** Monitoring staff measure each grant's monitoring needs using a system of pre-determined evaluation criteria. The criteria help assess the recipient and potential challenges to the success of the grant award.

2. **Monitoring Selection and Scheduling:** Monitoring staff make selection and scheduling decisions in accordance with applicable statutory requirements, such as the Homeland Security Act of 2002, as amended (hereafter "HSA") and consider the results of the monitoring assessment process.

3. **Monitoring Activities:** Monitoring activities include cash analysis, desk reviews, and site visits. Grants Management Specialists are responsible for conducting quarterly or semi-annual reviews of all grants via cash analysis. Desk reviews and site visits are additional monitoring activities conducted on grants where the monitoring assessment process identified the need for additional monitoring and validated the use of FEMA resources for these activities.

4. **Post-Monitoring Actions:** Monitoring staff may follow up with recipients via post-monitoring actions based on the outcomes of monitoring activities. Post-monitoring actions include conducting additional monitoring; reviewing Corrective Action Plans (CAP) and monitoring the progress of CAP deliverables; documenting the resolution of identified corrective actions and issues; providing TA and recipient training; and debt collection.

In addition to the monitoring guidance outlined above, section 2022(a)(2)(A) of the HSA mandates the frequency of monitoring activities for applicable preparedness grants. The applicable section of the HSA reads as follows:

> *Not less than once every 2 years, the Administrator shall conduct, for each state and high-risk urban area receiving a grant administered by the Department, a programmatic and financial review of all grants awarded by the Department to prevent, prepare for, protect against, or respond to natural disasters, acts of terrorism, or other man-made disasters, excluding assistance provided under section 203, title IV, or title V of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5133, 5170 et seq., and 5191 et seq.).*

HSGP (including SHSP, UASI, and OPSG), NSGP, TSGP, PSGP, and the EMPG Program are subject to HSA monitoring requirements. The IPR Program, IBSGP, and THSGP are *not* subject to HSA monitoring requirements.

6.1.3. STANDARD MONITORING ACTIVITY: CASH ANALYSIS

Through cash analysis, a Grants Management Specialist assesses and reports on the recipients' cash-on-hand, expenditures, and unliquidated obligations; gauges potential cost share shortfalls and cash on hand issues; and monitors spend down activities within the POP. The analysis reconciles and compares grant disbursement records with the recipient submitted FFR. This process identifies recipients that may require additional monitoring due to issues identified with drawdowns or FFR submissions.

6.1.4. ENHANCED MONITORING ACTIVITIES: DESK REVIEW, SITE VISIT

Desk reviews and site visits are two forms of additional monitoring that FEMA conducts on a recipient. Table 6 defines the key differences and similarities.

Table 6: Enhanced Financial Monitoring Activities (Desk Review and Site Visit)

Attribute	Desk Review	Site Visit
Location/ Logistics	A detailed, paper-based review and evaluation conducted at a FEMA office. Desk reviews do not require travel.	A visit by FEMA grants management staff conducted at the site of the recipient's operations and/or selected performance sites. Site visits may require travel.
Materials Reviewed	Required reports, correspondence, and other documentation, including policies and procedures, to substantiate compliance. Additional documentation available remotely may include information available through the grant file, financial reports, interviews, and other documentation and correspondence to verify compliance.	Includes documents listed under the desk review in addition to all applicable documents and required reports necessary to assess recipient capability and progress, validate records, and substantiate compliance with laws, regulations, and policies.
Goal of Monitoring Activity	The goals of FEMA's financial desk review monitoring activities are, as applicable, to: ▪ Review grant files to verify compliance, conduct interviews to confirm adherence to approved program plans, and confirm equipment acquisition, allowable use, and inventory controls; ▪ Document that recipient institutions possess adequate internal controls, policies, processes, and systems to manage FEMA grants effectively; ▪ Assist the recipient with the grant process and provide guidance to improve recipient administrative efficiencies;	The goals of FEMA's financial site visit monitoring activities are, as applicable, to: ▪ Review grant files to verify compliance, conduct interviews to confirm adherence to approved program plans, and confirm equipment acquisition, allowable use, and inventory controls; ▪ Document that recipient institutions possess adequate internal controls, policies, processes, and systems to manage FEMA grants effectively; ▪ Assist the recipient with the grant process and provide guidance to improve recipient administrative efficiencies;

Attribute	Desk Review	Site Visit
	▪ Identify and analyze relevant problems that might prevent the program from achieving its internal and external objectives; and ▪ Provide TA.	▪ Identify and analyze relevant problems that might prevent the program from achieving its internal and external objectives; and ▪ Provide TA.

6.1.5. PROGRAMMATIC MONITORING OVERVIEW AND APPROACH

Programmatic monitoring involves oversight throughout the award lifecycle for FEMA to verify that programs and projects undertaken by recipients are consistent with approved plans and comply with applicable laws, regulations, program guidance, and the terms and conditions of the award.

FEMA's monitoring approach complies with the monitoring requirements described in section 2022 of the HSA Programmatic monitoring also plays an important role in ensuring that FEMA preparedness grant funding builds and sustains capabilities at the SLTT levels that advance the Goal. Programmatic monitoring also is an opportunity for FEMA staff to build relationships with recipients and to work collaboratively to identify and mitigate factors that may impede programmatic performance.

The programs subject to section 2022 of the HSA and three additional programs (THSGP, IPR Program, and IBSGP) are included in this programmatic monitoring approach—meaning that all programs included in this manual are part of this programmatic monitoring approach.

FEMA uses a risk- and project-based programmatic monitoring framework for its preparedness grant programs that is designed for data-driven grants management, and which interacts seamlessly with other aspects of the grant lifecycle. FEMA uses monitoring as a vehicle to validate data previously self-reported by recipients in applications and reporting tools. FEMA does not utilize monitoring as a data collection tool in and of itself. By specializing monitoring in this way, FEMA avoids duplicative data collection, targets its resources more effectively, and provides stronger and more proactive TA to its recipients. The framework also comprehensively documents grant management decisions for resource allocation.

This programmatic monitoring approach establishes baseline monitoring of all open awards across the FEMA preparedness grant portfolio using a First Line Review (FLR). The FLR identifies recipients and awards with a high potential for noncompliance with regulations or failure to meet project objectives. The FLR uses quantifiable measures (criteria) to prioritize and rank recipients and awards according to identified risks that threaten the success of FEMA's preparedness grant awards. Results of this prioritization process determine which high-risk recipients and awards will receive advanced monitoring. Post-monitoring actions document and communicate findings and recommendations for resolution to the recipients and FEMA leadership and allow for increasingly cohesive programmatic and financial monitoring processes.

6.2. Case Studies and Use of Grant-Funded Resources During Real-World Incident Operations

Analyzing the use of grant-funded investments in real-world incidents will improve the ability of FEMA and its SLTT partners to assess the effectiveness of these investments and to better understand how grant funds support improvements in nationwide capability levels. Currently, FEMA conducts case

studies with a limited number of grant recipients each year to explore how jurisdictions prioritize grant investments based on risk and capability assessments, and the ways specific investments improve SLTT preparedness (see the Preparedness Grants Case Studies page on FEMA.gov). By accepting the award, the recipient agrees to participate in a case study or evaluation if requested. Recipients can also contact FEMA-PreparednessGrantEvaluation@fema.dhs.gov if interested in volunteering to participate in a case study.

6.3. Termination of the Federal Award

Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 sets forth a term and condition entitled "Termination of a Federal Award." The termination provision condition listed below applies to the grant award and the term and condition in Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 does not

6.3.1. TERMINATION OF THE FEDERAL AWARD BY FEMA

FEMA may terminate the federal award in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

- If the recipient or subrecipient fails to comply with the terms and conditions of the federal award.
- With the consent of the recipient, in which case FEMA and the recipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
- If the federal award no longer effectuates the program goals or agency priorities. Under this provision, FEMA may terminate the award for these purposes if any of the following reasons apply:
    - If DHS/FEMA, in its sole discretion, determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;
    - If DHS/FEMA, in its sole discretion, determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;
    - If DHS/FEMA, in its sole discretion, determines that the design of the grant program is flawed relative to program goals or agency priorities;
    - If DHS/FEMA, in its sole discretion, determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;
    - If DHS/FEMA, in its sole discretion, changes or re-evaluates the goals or priorities of the grant program and determines that the award will be ineffective at achieving the updated program goals or agency priorities; or
    - For other reasons based on program goals or agency priorities described in the termination notice provided to the recipient pursuant to 2 C.F.R. § 200.341.
    - If the awardee falls out of compliance with the Agency's statutory or regulatory authority, award terms and conditions, or other applicable laws.

6.3.2. TERMINATION OF A SUBAWARD BY THE PASS-THROUGH ENTITY

The pass-through entity may terminate a subaward in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

- If the subrecipient fails to comply with the terms and conditions of the Federal award.
- With the consent of the subrecipient, in which case the pass-through entity and the subrecipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
- If the pass-through entity's award has been terminated, the pass-through recipient will terminate its subawards.

6.3.3. TERMINATION BY THE RECIPIENT OR SUBRECIPIENT

The recipient or subrecipient may terminate the federal award in whole or in part for the following reason identified in 2 C.F.R. § 200.340: Upon sending FEMA or pass-through entity a written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if FEMA or pass-through entity determines that the remaining portion of the federal award will not accomplish the purposes for which the federal award was made, FEMA or the pass-through entity may terminate the federal award in its entirety.

6.3.4. IMPACTS OF TERMINATION

- When FEMA terminates the federal award prior to the end of the period of performance due to the recipient's material failure to comply with the terms and conditions of the Federal award, FEMA will report the termination in SAM.gov in the manner described at 2 C.F.R. § 200.340(c).
- When the federal award is terminated in part or its entirety, FEMA or the pass-through entity and the recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. §§ 200.344 and 200.345.

6.3.5. NOTIFICATION REQUIREMENTS

FEMA or the pass-through entity must provide written notice of the termination in a manner consistent with 2 C.F.R. § 200.341. The Federal award will be terminated on the date of the notification unless stated otherwise in the notification.

6.3.6. OPPORTUNITIES TO OBJECT AND APPEALS

Where applicable, when FEMA terminates the Federal award, the written notification of termination will provide the opportunity and describe the process to object and provide information challenging the action, pursuant to 2 C.F.R. § 200.342.

6.3.7. EFFECTS OF SUSPENSION AND TERMINATION

The allowability of costs to the recipient or subrecipient resulting from financial obligations incurred by the recipient or subrecipient during a suspension or after the termination of a federal award are subject to 2 C.F.R. § 200.343.

6.4. Period of Performance Extensions

Extensions to the POP for programs addressed in this manual are allowed under limited circumstances. Extensions to the initial POP identified in the award will only be considered through formal, written requests to the recipient's FEMA Preparedness Officer or Program Manager and must contain specific and compelling justifications as to why an extension is required. Recipients are advised to coordinate with their FEMA Preparedness Officer or Program Manager as needed when preparing an extension request.

All extension requests must address the following:

1. The grant program, fiscal year, and award number;
2. Reason for the delay—including details of the legal, policy, or operational challenges that prevent the final outlay of awarded funds by the deadline;
3. Current status of the activity(ies);
4. Approved POP termination date and new project completion date;
5. Amount of funds drawn down to date;
6. Remaining available funds, both federal and, if applicable, non-federal;
7. Budget outlining how remaining federal and, if applicable, non-federal funds will be expended;
8. Plan for completion, including milestones and timeframes for achieving each milestone and the position or person responsible for implementing the plan for completion; and
9. Certification that the activity(ies) will be completed within the extended POP without any modification to the original statement of work, as described in the IJ and as approved by FEMA.

Extension requests will be granted only due to compelling legal, policy, or operational challenges. Extension requests will only be considered for the following reasons:

- Contractual commitments by the recipient or subrecipient with vendors prevent completion of the project within the existing POP;
- The project must undergo a complex environmental review that cannot be completed within the existing POP;
- Projects are long-term by design, and therefore acceleration would compromise core programmatic goals; or
- Where other special or extenuating circumstances exist.

Recipients should submit all proposed extension requests to FEMA for review and approval at least 120 days before the end of the POP to allow sufficient processing time. Extensions are typically granted for no more than a six-month period. Recipients are advised to coordinate with their FEMA Preparedness Officer or Program Manager as needed when preparing an extension request.

Recipients should refer to the corresponding chapter of this manual for program-specific details related to POP extensions.

6.5. Conflicts of Interest in the Administration of Federal Awards or Subawards

For conflicts of interest under grant-funded procurements and contracts, refer to the section on Procurement Integrity in this manual and 2 C.F.R. §§ 200.317 – 200.327.

To eliminate and reduce the impact of conflicts of interest in the subaward process, recipients and pass-through entities must follow their own policies and procedures regarding the elimination or reduction of conflicts of interest when making subawards. Recipients and pass-through entities are also required to follow any applicable federal or SLTT statutes or regulations governing conflicts of interest in the making of subawards.

The recipient or pass-through entity must disclose to the respective Preparedness Officer or Program Manager, in writing, any real or potential conflict of interest that may arise during the administration of the federal award, as defined by the federal or SLTT statutes or regulations or their own existing policies, within five calendar days of learning of the conflict of interest. Similarly, subrecipients, whether acting as subrecipients or as pass-through entities, must disclose any real or potential conflict of interest to the recipient or next-level pass-through entity as required by the recipient or pass-through entity's conflict of interest policies, or any applicable federal or SLTT statutes or regulations.

Conflicts of interest may arise during the process of FEMA making a federal award in situations where an employee, officer, or agent, any members of their immediate family or their partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, subapplicant, recipient, subrecipient, or FEMA employee.

6.6. Procurement Integrity

When purchasing under a FEMA award, recipients and subrecipients must comply with the federal procurement standards in 2 C.F.R. §§ 200.317 – 200.327. To assist with determining whether an action is a procurement or instead a subaward, please consult 2 C.F.R. § 200.331.

For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA's Procurement Disaster Assistance Team (PDAT). Additional resources, including the Procurement Under Grants Policy Guide (PUGPG) an upcoming trainings schedule can be found on the PDAT Website: https://www.fema.gov/grants/procurement.

Under 2 C.F.R. § 200.317, when procuring property and services under a federal award, States (including territories) and Indian Tribes must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states and Indian Tribes must now follow 2 C.F.R. § 200.322 regarding domestic preferences for Procurements and 2 C.F.R. § 200.327 regarding required contract provisions. States, but not Indian Tribes, must also follow 2 C.F.R. § 200.323 regarding procurement of recovered materials.

Local government and nonprofit recipients or subrecipients must have and use their own documented procurement procedures that reflect applicable State, Local, Tribal, and Territorial (SLTT) laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200.

6.6.1. IMPORTANT CHANGES TO PROCUREMENT STANDARDS IN 2 C.F.R. PART 200

On April 22, 2024, OMB updated various parts of Title 2 of the Code of Federal Regulations, among them the procurement standards. These revisions apply to all FEMA awards with a federal award date or disaster declaration date on or after October 1, 2024, unless specified otherwise. The changes include updates to the federal procurement standards, which govern how FEMA award recipients and subrecipients must purchase under a FEMA award.

More information on OMB's revisions to the federal procurement standards can be found in Purchasing Under a FEMA Award: 2024 OMB Revisions Fact Sheet.

6.6.2. COMPETITION AND CONFLICTS OF INTEREST

2 C.F.R. § 200.319(b), applicable to local government and nonprofit recipients or subrecipients, requires that contractors that develop or draft specifications, requirements statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a recipient or subrecipient develop its grant application, project plans, or project budget. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the recipient or subrecipient.

Under this prohibition, unless the recipient or subrecipient solicits for and awards a contract covering both development and execution of specifications (or similar elements as described above), and this contract was procured in compliance with 2 C.F.R. §§ 200.317 – 200.327, federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with federal grant funds, including pre-award costs, such as grant writer fees, as well as post- award costs, such as grant management fees.

In addition to organizational conflicts of interest, situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business;
- Requiring unnecessary experience and excessive bonding;
- Noncompetitive pricing practices between firms or between affiliated companies;
- Noncompetitive contracts to consultants that are on retainer contracts;
- Specifying only a "brand name" product instead of allowing "an equal" product to be offered and describing the performance or other relevant requirements of the procurement; and
- Any arbitrary action in the procurement process.

Under 2 C.F.R. § 200.318(c)(1), local government and nonprofit recipients or subrecipients are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. **No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if he or she has a real or apparent conflict of interest. Such conflicts of interest would arise when the employee, officer or agent, any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the parties indicated**

herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the recipient or subrecipient may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, the recipient or subrecipient may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The recipient's or subrecipient's standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents.

Under 2 C.F.R. 200.318(c)(2), if the local government and nonprofit recipient or subrecipient has a parent, affiliate, or subsidiary organization that is not a SLTT government, the recipient or subrecipient must also maintain written standards of conduct covering organizational conflicts of interest. Organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the recipient or subrecipient is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The recipient or subrecipient must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

6.6.3. SUPPLY SCHEDULES AND PURCHASING PROGRAMS

Generally, a recipient or subrecipient may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

6.6.4. PROCUREMENT DOCUMENTATION

Per 2 C.F.R. § 200.318(i), local government and nonprofit recipients or subrecipients are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and Indian Tribes are reminded that in order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g).

Examples of the types of documents that would cover this information include, but are not limited to:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

6.7. Records Retention

6.7.1. RECORD RETENTION PERIOD

Financial records, supporting documents, statistical records, and all other non-Federal entity records pertinent to a federal award generally must be maintained for at least three years from the date the

final FFR is submitted. See 2 C.F.R. § 200.334. Further, if the recipient does not submit a final FFR and the award is administratively closed, FEMA uses the date of administrative closeout as the start of the general record retention period.

The record retention period may be longer than three years or have a different start date in certain cases.

6.7.2. TYPES OF RECORDS TO RETAIN

FEMA requires that recipients and subrecipients maintain the following documentation for federally funded purchases:

- Specifications
- Solicitations
- Competitive quotes or proposals
- Basis for selection decisions
- Purchase orders
- Contracts
- Invoices
- Canceled checks

6.8. Actions to Address Noncompliance

Non-federal entities receiving financial assistance funding from FEMA are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R. §§ 200.208 and 200.339. FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R. § 200.339, or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to 44 C.F.R. Parts 7 and 19 or other applicable regulations.

If the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA may take other remedies allowed under 2 C.F.R. § 200.339.

6.9. Audits

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS Office of the Inspector General (OIG), the GAO, the pass-through entity, or independent auditing firms for single audits, and may cover activities and costs incurred under the award. Auditing agencies such

as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award.

6.9.1. SINGLE AUDIT REPORT

A recipient expending $1,000,000 or more in federal awards (as defined by 2 C.F.R. § 200.1) during its FY must undergo an audit. This may be either a single audit complying with 2 C.F.R. § 200.514 or a program-specific audit complying with 2 C.F.R. §§ 200.501 and 200.507. Audits must follow 2 C.F.R. Part 200, Subpart F, 2 C.F.R. § 200.501, and the U.S. Government Accountability Office (GAO) Generally Accepted Government Auditing Standards.

6.10. Reporting Issues of Fraud, Waste, and Abuse

Recipients, subrecipients, State Administrative Agencies (SAAs), and any other applicable stakeholder at any time may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct to the OIG Hotline. The toll-free numbers to call are 1 (800) 323-8603, and TTY 1 (844) 889-4357.

6.11. Payment Information

Payment requests are submitted through FEMA GO for awards obligated in FY 2024 and going forward. For awards obligated prior to FY 2024 in the ND Grants System, the payment request is submitted through PARS.

6.11.1. INSTRUCTIONS TO GRANT RECIPIENTS PURSUING PAYMENTS

FEMA reviews all grant payments and obligations to ensure allowability in accordance with 2 C.F.R. § 200.305. These measures ensure funds are disbursed appropriately while continuing to support and prioritize communities who rely on FEMA for assistance. Once a recipient submits a payment request, FEMA will review the request. If FEMA approves a payment, recipients will be notified by FEMA GO and the payment will be delivered pursuant to the recipients SAM.gov financial information. If FEMA disapproves a payment, FEMA will inform the recipient.

6.11.2. PROCESSING AND PAYMENT TIMELINE

FEMA must comply with regulations governing payments to grant recipients. See 2 C.F.R. § 200.305. For grant recipients other than States, 2 C.F.R. § 200.305(b)(3) stipulates that FEMA is to make payments on a reimbursement basis within 30 days after receipt of the payment request, unless FEMA reasonably believes the request to be improper. For state recipients, 2 C.F.R. § 200.305(a) instructs that federal grant payments are governed by Treasury-State Cash Management Improvement Act (CMIA) agreements ("Treasury-State agreement") and default procedures codified at 31 C.F.R. part 205 and Treasury Financial Manual (TFM) 4A-2000, "Overall Disbursing Rules for All Federal Agencies." *See* 2 C.F.R. § 200.305(a).

Treasury-State agreements generally apply to "major federal assistance programs" that are governed by 31 C.F.R. part 205, subpart A and are identified in the Treasury-State agreement. 31 C.F.R. §§ 205.2, 205.6. Where a federal assistance (grant) program is not governed by subpart A, payment and funds transfers from FEMA to the state are subject to 31 C.F.R. part 205, subpart B. Subpart B requires FEMA to "limit a funds transfer to a state to the minimum amounts needed by the state and must time the disbursement to be in accord with the actual, immediate cash requirements of the state in carrying out a federal assistance program or project. The timing and amount of funds

transfers must be as close as is administratively feasible to a state's actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs." 31 C.F.R. § 205.33(a). Nearly all FEMA grants are not "major federal assistance programs." As a result, payments to states for those grants are subject to the "default" rules of 31 C.F.R. part 205, subpart B.

If additional information is needed, a request for information will be issued by FEMA to the recipient; recipients are strongly encouraged to respond to any additional FEMA request for information inquiries within three business days. If an adequate response is not received, the request may be denied, and the entity may need to submit a new reimbursement request; this will re-start the 30-day timeline.

6.11.3. SUBMISSION PROCESS

All non-disaster grant program reimbursement requests must be reviewed and approved by FEMA prior to drawdowns.

For all non-disaster reimbursement requests (regardless of system), please ensure submittal of the following information:

1. Grant ID / Award Number
2. Total amount requested for drawdown
3. Purpose of drawdown and timeframe covered (must be within the award performance period)
4. Subrecipient Funding Details (if applicable)
   - Is funding provided directly or indirectly to a subrecipient?
     - If **no,** include statement "This grant funding is not being directed to a subrecipient."
   - If **yes**, provide the following details:
     - The name, mission statement, and purpose of each subrecipient receiving funds, along with the amount allocated and the specific role or activity being reimbursed.
     - Whether the subrecipient's work or mission involves supporting aliens, regardless of whether FEMA funds support such activities.
     - Whether the payment request includes an activity involving support to aliens.
     - Whether the subrecipient has any diversity, equity, and inclusion practices.
5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under 2 CFR Part 200 and in compliance with the grant's NOFO, award terms, and applicable federal regulations.

6.12. Whole Community Preparedness

Preparedness is a shared responsibility that calls for the involvement of everyone—not just the government—in preparedness efforts. By working together, everyone can help keep the nation safe from harm and help keep it resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics. Whole community includes, but is not limited to:

- Individuals and families, including those with disabilities and others with access and functional needs;

- Businesses;
- Faith-based and community organizations;
- Nonprofit groups;
- Schools and academia;
- Media outlets; and
- All levels of government, including SLTT and federal partners.

The phrase “whole community” often appears in preparedness materials, as it is one of the guiding principles. It means two things:

- Involving people in the development of national preparedness documents; and
- Ensuring their roles and responsibilities are reflected in the content of the materials.

By engaging whole community stakeholders, preparedness grant recipients can develop and promote a suite of well-targeted solutions for individuals and communities to adopt. Recipients should coordinate preparedness initiatives with whole community partners to efficiently apply federal funding to reach the goal of individual and community resilience.

7. Resources

7.1. Department of Homeland Security/FEMA Provided Training and Education

FEMA offers tuition-free training and education programs and courses through several providers including the Center for Domestic Preparedness (CDP), National Disaster and Emergency Management University (NDEMU), and NTED's Training Partner Program (TPP). TPP includes the Center for Homeland Defense and Security, National Domestic Preparedness Consortium (NDPC), Rural Domestic Preparedness Consortium (RDPC),National Cybersecurity Preparedness Consortium (NCPC), and training partners through the Continuing Training Grants (CTG) program.

7.2. Training Not Provided by the Department of Homeland Security/FEMA

Trainings not provided by DHS/FEMA include courses that are either state-sponsored or federal-sponsored (non-DHS/FEMA), coordinated and approved by the SAA or their designated Training Point of Contact (TPOC), and fall within the FEMA mission scope to prepare SLTT personnel to prevent, protect against, mitigate, and respond to acts of terrorism or catastrophic events. These trainings often pertain to the HSGP and THSGP.

- *State Sponsored Courses*. These courses are developed for and/or delivered by institutions or organizations other than federal entities or FEMA and are sponsored by the SAA or their designated TPOC.

- *Joint Training and Exercises with the Public and Private Sectors*. These courses are sponsored and coordinated by private sector entities to enhance public-private partnerships for training personnel to prevent, protect against, mitigate, and respond to acts of terrorism or catastrophic events. In addition, states, territories, Tribal Nations, and high-risk urban areas are encouraged to incorporate the private sector in government-sponsored training and exercises.

Additional information on both FEMA provided training and other federal and state training can be found at firstrespondertraining.gov.

7.3. Training Information Reporting System ("Web-Forms")

Web-Forms is an electronic data management system built to assist recipients and federal agencies with submitting non-NTED provided training courses for inclusion in the State/Federal-Sponsored Course Catalog through electronic forms. The information collected is used in a two-step review process to ensure the training programs adhere to the intent of the guidance and the course content is structurally sound and current. As these programs may be delivered nationwide, it is vital to ensure each training program's viability and relevance to the Homeland Security mission. Reporting training activities through Web-Forms is not required under present funding. However, the system remains available and can be accessed through the Web-Forms section of the FEMA National Preparedness Course Catalog to support recipients in their own tracking of training deliveries. Users need to request First Responder Training System (FRTS) Admin rights from NTED to access the Web-Forms.

7.4. FEMA's National Preparedness Course Catalog

Recipients are also encouraged to utilize FEMA's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes CDP, NDEMU, TPP, CTG, NDPC, RDPC, and other partners.

The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal and SLTT audiences. The catalog can be accessed at the NTED National Preparedness Course Catalog page on firstrespondertraining.gov.

Some exercise and training activities require EHP Review, including those that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on training requirements and EHP review can be found online at the Environmental & Historic Preservation Guidance for FEMA Grant Applications page on FEMA.gov.

7.5. Exercises

Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at the HSEEP page on FEMA.gov.

7.6. Planning Assistance

FEMA's NPD offers TA that is designed to provide recipients and subrecipients with specialized expertise to improve and enhance the continuing development of state and local emergency management across the five mission areas of the Goal and across all core capabilities. TA provides the opportunity to engage emergency managers, emergency planners, and appropriate decision-makers in open discussion of options to improve plans and planning considering their jurisdiction's needs. Although there is no direct cost to approved jurisdictions for FEMA TA, jurisdictions are expected to invest staff resources and take ownership of the resulting products and tools.

TA deliveries combine current emergency management best practices with practical consideration of emerging trends, through discussion facilitated by FEMA contract specialists and with the support of FEMA Region operational specialists. Additionally, peer-to-peer representation may also be included from other jurisdictions that have recently addressed the same planning issue. The TA request form can be accessed at the NIMS Implementation and Training page on FEMA.gov

7.7. Training Information

States, territories, tribal entities, and high-risk urban areas do not need to request approval from FEMA for personnel to attend non-DHS/FEMA training if the training is coordinated with and approved by the state, territory, tribal, or high-risk urban area TPOC and falls within the FEMA mission scope and the jurisdiction's Emergency Operations Plan (EOP).

FEMA will conduct periodic reviews of all SLTT entities, and high-risk urban area training funded by FEMA. These reviews may include requests for all course materials and physical observation of, or participation in, the funded training. If these reviews determine that courses are outside the scope of this guidance, recipients will be asked to repay grant funds expended in support of those efforts.

7.8. Weblinks

- U.S. Department of Transportation (DOT) "RAISE" grants for National Infrastructure Investments may include funding to support roads, bridges, transit, rail, ports, or intermodal transportation. See the RAISE Discretionary Grants page on Transportation.gov for more information.

- Cybersecurity Assessment Evaluation and Standardization, Cyber Resilience Review, Cyber Infrastructure Survey, and other resources are available via CISA. See the Cyber Resource Hub for additional information.

7.9. Emergency Management Accreditation Program

States can encourage their local jurisdictions to pursue assessment and accreditation under the Emergency Management Accreditation Program (EMAP). EMAP's assessment and accreditation of emergency management organizations against consensus-based, American National Standards Institute (ANSI)-certified standards allows for standardized benchmarking of critical functions necessary for an emergency management organization to meet the core capabilities identified in the Goal. Additional information on the EMAP Standard is available on the EMAP website.

8. Homeland Security Grant Program and Tribal Homeland Security Grant Program

8.1. Alignment to the National Preparedness System (Homeland Security Grant Program, Tribal Homeland Security Grant Program)

The Nation uses the National Preparedness System to build, sustain, and deliver core capabilities to achieve the Goal. HSGP and THSGP recipients use the National Preparedness System to support their efforts to build, sustain, and deliver these core capabilities, which are essential for each of the five mission areas outlined in the Goal. The components of the National Preparedness System are Identifying and Assessing Risk, Estimating Capability Requirements, Building and Sustaining Capabilities, Planning to Deliver Capabilities, Validating Capabilities, and Reviewing and Updating. Additional information on the National Preparedness System is available at the National Preparedness System page on FEMA.gov.

As the National Preparedness System matures, we are getting better data on our capabilities as a Nation that can be used to drive our focus and our resources at all levels. States, Tribal Nations, and territories provide annual data on their proficiency across 32 core capabilities through the THIRA, Stakeholder Preparedness Review (SPR), exercise and real world After-Action Reports (AAR), and other preparedness data. These data feed into the National Preparedness Report and form a shared national picture of needs relative to capability gaps, including what threats and hazards are posing the greatest risks and what core capabilities are most in need of improvement or sustainment. Communities and federal agencies alike use these data to prioritize, synchronize, and guide programs and activities to build and sustain capabilities. FEMA requires recipients to prioritize grant funding to demonstrate how investments support identified national priorities (for HSGP only) and building capability, closing capability gaps, or sustaining capabilities as defined by Comprehensive Preparedness Guide (CPG) 201: THIRA/SPR Guide, Third Edition. Analytic results help shape prioritization decisions at FEMA and across the nation to make sure we are focusing our time and our resources in the right areas.

The HSGP and THSGP provide financial support to SLTT jurisdictions to help them build, sustain, and deliver core capabilities identified in the Goal. Key focus areas and requirements of both the HSGP and THSGP are to prevent terrorism and other catastrophic events and to prepare the Nation for the threats and hazards that pose the greatest risk to the security of the United States and Tribal Nations, including risks along the nation's borders. When applicable, funding should support deployable assets that can be used nationwide through automatic assistance and mutual aid agreements, including, but not limited to, the EMAC.

The HSGP and THSGP support investments that improve the ability of jurisdictions nationwide to:

- Prevent a threatened or an actual act of terrorism;
- Protect citizens, residents, visitors, and assets against the threats that pose the greatest risk to the security of the United States;
- Mitigate the loss of life and property by lessening the impact of future catastrophic events; and/or
- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident.

8.2. Reporting on the Implementation of the National Preparedness System (Homeland Security Grant Program, Tribal Homeland Security Grant Program)

8.2.1. IDENTIFYING AND ASSESSING RISK AND ESTIMATING CAPABILITY REQUIREMENTS

HSGP: By Dec. 31 each year, states, territories, and high-risk urban area HSGP recipients are required to complete an SPR for capability targets that most challenge the 32 core capabilities. Additionally, the SPR must be compliant with CPG 201, Third Edition. Recipients should contact fema-spr@fema.dhs.gov for the list of required capability targets. Additionally, every three years recipients are required to complete a THIRA. In 2020, jurisdictions began the requirement to respond to a series of planning-related questions as part of the THIRA/SPR.

THSGP: THSGP recipients are required to complete a THIRA every three years. Tribal Nations with open THSGP awards must update their SPR inputs and Secondary Assessments (described in Section 8.2.4 "Planning to Deliver Capabilities" and Section 8.2.3 "National Incident Management System Implementation") for activities completed in each respective calendar year (CY) throughout the POP, starting the CY *after* funding is awarded.

New THSGP recipients are required to complete the THIRA, SPR, and Secondary Assessments by Dec. 31 of the year *following* award issuance. New THSGP recipients are recipients that have *not* received THSGP funding in the past three years. The THIRA/SPR must address all 32 core capabilities and be compliant with the CPG 201, Third Edition. When applying for THSGP funding, Tribal Nations that were awarded THSGP funding during the previous two years are expected to prioritize and align grant funding investments in building and sustaining capabilities as identified in their THIRA and SPR.

For additional guidance on the THIRA/SPR, please refer to CPG 201, Third Edition.

Reporting

- States, Tribal Nations (with the exception of new THSGP recipients as noted above), and territories will submit their THIRA and SPR through the URT on the Preparedness Toolkit no later than Dec. 31 of the applicable year (every three years for THIRA and each year for SPR) for which the recipient has an open award.
    - If a THSGP recipient has completed closeout for their THSGP grant award POP, they do not have to submit the THIRA/SPR as the requirement does not apply to closed awards.
- High-risk urban areas that receive UASI funding will submit their SPR through the URT on Preparedness Toolkit no later than Dec. 31 for the years they have UASI open grants. If a UASI recipient has completed closeout for their UASI grant award POP, they do not have to submit a THIRA/SPR as the requirement is not applicable to closed grant awards. Although UASIs that have completed closeout for the award POP are not required to complete a THIRA/SPR, it is encouraged.
- Calendar year 2022 was the start of the new three-year THIRA/SPR cycle and baseline assessment year for existing recipients. Any new grant recipients for which the THIRA/SPR requirement applies will start their new three-year THIRA/SPR cycle and baseline assessment year in the year during which they apply. States, territories, and high-risk urban areas should

work collaboratively to create the most accurate THIRA and SPR possible. States, territories, and high-risk urban areas may share scenarios, targets, and assessed capabilities when appropriate.

- Please contact FEMA-SPR@fema.dhs.gov if you have questions.

8.2.2. BUILDING AND SUSTAINING CAPABILITIES

States, territories, and high-risk urban areas must prioritize and align SHSP and UASI grant funding investments in building and sustaining capabilities in areas that align with the national priorities in the annual HSGP NOFO, and capability gaps identified in their THIRA and SPR. Tribal Nations receiving THSGP funds must prioritize and align grant funding investments in building and sustaining capabilities as identified in their THIRA and SPR. When applying for THSGP funding, Tribal Nations that were awarded THSGP funding during the previous two years are expected to prioritize and align grant funding investments in building and sustaining capabilities as identified in their THIRA and SPR.

Reporting

Within the BSIR and as part of programmatic monitoring, recipients must describe how expenditures support building capability, closing capability gaps, or sustaining capabilities identified in the THIRA and SPR. Recipients must, on a project-by-project basis, check one of the following:

- Building a capability with HSGP or THSGP funding; and
- Sustaining a capability with HSGP or THSGP funding.

8.2.3. NATIONAL INCIDENT MANAGEMENT SYSTEM IMPLEMENTATION

Recipients receiving HSGP or THSGP funding are required to implement NIMS. HSGP and THSGP recipients must use standardized resource management concepts for resource typing, credentialing, and an inventory to facilitate the effective identification, dispatch, deployment, tracking, and recovery of resources.

Reporting

- Recipients report in the applicable secondary NIMS assessment portion of the URT as part of their THIRA/SPR submission, as outlined in the HSGP or THSGP NOFO.

8.2.4. PLANNING TO DELIVER CAPABILITIES

HSGP and THSGP recipients shall develop and maintain, jurisdiction-wide, all threats and hazards EOPs consistent with CPG 101, Version 3.1 (CPG 101 v3.1), Developing and Maintaining Emergency Operations Plans (May 2025). For HSGP, recipients must update their EOPs at least once every two years. For THSGP, recipients must submit an EOP once during the POP.

Reporting

- Recipients report EOP compliance with CPG 101 v3.1 by completing the secondary CPG 101 v3.1 assessment portion of the URT as part of their THIRA/SPR submission.

8.2.5. VALIDATING CAPABILITIES

All HSGP and THSGP recipients will develop and maintain a progressive exercise program consistent with HSEEP guidance in support of the National Exercise Program (NEP). THSGP recipients are required to develop and maintain this program regardless of whether the Tribal Nation planned to use THSGP funding for exercises. The NEP serves as the principal exercise mechanism for examining national preparedness and measuring readiness. The NEP is a two-year cycle of exercises across the nation that validates capabilities in all preparedness mission areas. The two-year NEP cycle is guided by Principals' Strategic Priorities, established by the National Security Council, and informed by preparedness data from jurisdictions across the Nation.

To develop and maintain a progressive exercise program consistent with HSEEP and in support of the NEP, recipients should engage senior leaders and other whole community stakeholders to identify preparedness priorities. These priorities should be informed by various factors, including jurisdiction-specific threats and hazards (i.e., the THIRA); areas for improvement identified by real-world events and exercises; external requirements such as state or national preparedness reports, homeland security policy, and industry reports; and accreditation standards, regulations, or legislative requirements. Recipients should document these priorities and use them to deploy a schedule of preparedness events in a multi-year Integrated Preparedness Plan (IPP). Information related to Integrated Preparedness Planning Workshops (IPPWs) can be found on the HSEEP page on FEMA.gov and the Preparedness Toolkit.

The NEP provides exercise sponsors the opportunity to receive exercise design and delivery assistance, tools and resources, enhanced coordination, and the ability to directly influence and inform policy and preparedness programs. If you have any questions, or would like to request assistance through the NEP, please visit the NEP website on the Exercises page on FEMA.gov, or reach out to the NEP directly at NEP@fema.dhs.gov.

Reporting

- Recipients must have a current multi-year IPP that identifies preparedness priorities and activities. The current multi-year IPP must be submitted to hseep@fema.dhs.gov before Jan. 31 of each year:
    - Recipients are encouraged to enter their exercise information into the Preparedness Toolkit.
- Recipients must submit AARs/Improvement Plans (IPs) to hseep@fema.dhs.gov and indicate which fiscal year funds were used (if applicable).
- Submission of AAR/IPs must take place within 90 days following completion of the single exercise or progressive series:
    - Recipients are encouraged to submit AAR/IPs reflecting tabletop exercises that validate critical plans or those reflecting large-scale functional or full-scale exercises that took place at the state, territorial, tribal, or urban area level. Recipients are discouraged from submitting AAR/IPs specific to local jurisdictions that reflect drills;
    - If a recipient endures a significant real-world incident during the CY that delays or prevents conduct of a grant-funded exercise, they can submit the AAR from that event in place of the exercise AARs. Jurisdictions submitting real world AARs should include an explanation with the AAR submission to hseep@fema.dhs.gov; and

- Recipients can access a sample AAR/IP template on the Improving Planning Templates page on the Preparedness Toolkit.

8.3. Funding Guidelines (Homeland Security Grant Program, Tribal Homeland Security Grant Program)

Recipients must comply with all the requirements in 2 C.F.R. Part 200 (*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*). In general, recipients should consult with their FEMA HQ Preparedness Officer prior to making any investment that does not clearly meet the allowable expense criteria. Funding guidelines support four of the five mission areas—Prevention, Protection, Mitigation, and Response—and associated core capabilities within the Goal. While Recovery is part of the Goal, it is not explicitly part of the HSGP and THSGP. Allowable investments made in support of the national priorities, as well as other capability-enhancing projects must have a nexus to terrorism preparedness and fall into the categories of planning, organization, exercises, training, or equipment, aligned to building capability, closing capability gaps, and/or sustaining capabilities, as defined by CPG 201, Third Edition. Recipients are encouraged to use grant funds for evaluating grant-funded project effectiveness and return on investment. FEMA encourages recipients to provide the results of that analysis to FEMA.

8.4. Allowable Cost (Homeland Security Grant Program)

8.4.1. MULTIPLE PURPOSE OR DUAL-USE OF FUNDS (STATE HOMELAND SECURITY PROGRAM AND URBAN AREA SECURITY INITIATIVE)

For both SHSP and UASI, many activities that support the achievement of core capabilities related to the national priorities and terrorism preparedness may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. However, all SHSP and UASI funded projects must assist recipients and subrecipients in achieving core capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism per section 2008(c) of the HSA (6 U.S.C. § 609(c)).

8.4.2. ORGANIZATIONAL ACTIVITIES

Personnel Costs

In addition to the personnel cost allowability detailed in the HSGP NOFO, HSGP (SHSP, UASI) funds may not be used to support the hiring of any personnel to fulfill traditional public health and safety duties nor to supplant traditional public health and safety positions and responsibilities. **HSGP (SHSP, UASI, OPSG) funds will be used to supplement existing funds and will NOT replace (supplant) funds that have been appropriated and/or budgeted for the same purpose**. Applicants or recipients may be required to supply documentation certifying that a reduction in non-federal resources occurred for reasons other than the receipt or expected receipt of federal funds.

8.4.3. 28 C.F.R. PART 23 GUIDANCE

FEMA requires that any IT system funded or supported by HSGP funds comply with 28 C.F.R. Part 23, Criminal Intelligence Systems Operating Policies if this regulation is determined to be applicable.

8.5. Fusion Centers (Homeland Security Grant Program)

A critical component of the national response to the 9/11 terrorist attacks was the development of a national-level, decentralized, and coordinated terrorism-related information sharing environment (ISE). State and local governments, supported by federal investments from DHS, DOJ, Department of Health and Human Services (HHS), and other federal agencies of the national ISE. This National Network, composed of 80 state and major urban area fusion centers, collaborates and shares information with partners from all levels of government and the private sector, as well as other field-based information sharing partners, including High-Intensity Drug Trafficking Areas (HIDTA), Regional Information Sharing Systems (RISS) Centers, Joint Terrorism Task Forces (JTTF), major city/county intelligence units, and real-time crime analysis centers, among others.

National Network participation in the Nationwide Suspicious Activity Reporting Initiative (NSI) enables fusion centers to identify, receive and analyze Suspicious Activity Reports (SAR) and other tips/leads from frontline public safety personnel, the private sector, and the public, and ensure the sharing of SARs with DHS and the FBI's JTTFs for further investigation. In addition to those activities identified in the National Prevention Framework, fusion centers are also required to collaborate with those intelligence, operational, analytic, investigative, and information-sharing focused entities to combat a wide array of threats—noted below—in support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism, targeted violence, and other threats. Such entities include, but are not limited to JTTFs, Area Maritime Security Committees (AMSC), Border Enforcement Security Task Forces, Integrated Border Enforcement Teams, HIDTAs, and RISS Centers as well as other federal intelligence, operational, analytic, and investigative entities. Applicants should describe their collaboration plan and proposed efforts in their required Fusion Center project as part of the Intelligence and Information Sharing National Priority.

Today's threats—including international and domestic terrorism, drugs, gangs, active shooters, targeted violence, transnational organized crime, and cyber—require federal, state, and local governments to leverage this national capacity to effectively respond to the evolving nature of the various national and homeland security threats confronting our Nation. Ultimately, timely identification and analysis of key indicators from local, state, and federal partners will enable all stakeholders to address threats and develop and implement data-driven strategies to prevent, protect against, mitigate, and respond effectively, while ensuring the protection of privacy, civil rights, and civil liberties.

To underscore the importance of the National Network as a critical component of our Nation's distributed homeland security and counterterrorism architecture, FEMA preparedness grants will continue to prioritize support for designated fusion centers and the maturation of the ISE. Fusion centers **must** prioritize the following capabilities to further enable and mature this national asset and strengthen the collective capacity to identify, collect, analyze, and share information, and to disseminate actionable and strategic intelligence to key stakeholders:

- **Addressing Threats**: Fusion centers provide a national level, decentralized, and coordinated ISE across all levels of government and disciplines that can be leveraged and applied to address threats to homeland security, national security, public safety, and/or public health, and especially those threats that may have little or no warning. Fusion centers should leverage and build upon their terrorism-focused analytic and information-sharing capabilities so they can be applied to address threats across the DHS mission space, including threats from both international terrorism and domestic violent extremists, threats to life and targeted violence, transnational organized criminal activity, cyber threats, and natural hazards, among others that require close collaboration with DHS operational, investigative, and analytic entities such as CBP,

ICE, United States Secret Service (USSS), CISA, the United States Coast Guard (USCG), and FEMA.

- **Analytic Capability**: Fusion centers must maintain strong analytic capabilities at tactical, operational, and strategic levels to address a wide array of threats or hazards that could have implications for homeland security or national security. These capabilities directly support operational, investigative, and information sharing efforts across all levels of government. These capabilities include, but are not limited to:
    - Building and sustaining a capable workforce of analysts who have the necessary experience and training; access to open source, unclassified and classified information, products, data, SAR; tips/leads and online/social media-based threats; as well as necessary services and technology to facilitate analytic capabilities and collaboration;
    - Assessing, evaluating, and deconflicting acts of targeted violence, threats to life, and other criminal or suspicious activity, to include potential indicators and behaviors, for potential connection to or implications for international or domestic terrorism, or other threats within the DHS mission space;
    - Providing analytic support and responses to requests for information from federal, state, and local partners during no notice threats, attacks, or incidents, as well as other planned events such as National Security Special Events (NSSEs);
    - Conducting threat assessments within their respective jurisdictions, including the identification of threats, intelligence gaps, and mitigation efforts;
    - Establishing, formalizing, and maintaining bi-directional information sharing with federal and other state agencies in accordance with jurisdictional authorities;
    - Leveraging available resources and capabilities to conduct target and event deconfliction in support of threat identification, officer safety, and information sharing.
    - Maintaining an ability to routinely support federal government efforts to watchlist terrorists and transnational organized crime actors; and
    - Appropriately planning for, and assessing/forecasting, prioritizing, and executing against both known and emerging threat vectors, and ensuring the safety and security of all operations, while protecting privacy, civil rights, and civil liberties.

Fusion centers should also consider their operational capacity when aligning manpower and resources in support of this capability (e.g., the ability to maintain watch and analytic support functions over a 24/7 operational tempo).

- **Technological Integration:** Access to data, information, and products is essential for fusion centers and the federal government to effectively identify, collect, analyze, and share information. Just as threats do not stop at jurisdictional borders, fusion centers must be able to effectively access and share appropriate information and data across jurisdictions, agencies, and disciplines. Fusion centers must **ensure and certify via the Fusion Center Assessment** they have the necessary technological capacity to access, analyze, and share information, including criminal intelligence and online/social media threat information, both within their jurisdictions, as well as with other fusion centers across the country and with the Federal Government through a variety of systems, databases, tools, and technologies that allow for federated searching and

data/information analysis that protects Personally Identifiable Information and includes appropriate security, privacy, civil rights, and civil liberties protections. This includes maintenance of the ability to collect, integrate, evaluate, and assess SAR, tips/leads, data resident in Computer Assisted/Aided Dispatch (CAD) and Records Management System (RMS), and online/social media-based threats from agencies across the jurisdiction. Such approaches should also address the evaluation and use of emerging capabilities, including social network analysis, federated search technology across CAD, RMS, and other data systems, complex data indexing, social media, open source, facial recognition, unmanned aircraft systems, geographic information systems (GIS), license plate reader technologies, and other artificial intelligence technologies.

- **Interagency Collaboration:** Fusion centers must maintain strong partnerships to enable intelligence, operational, investigative, and analytic collaboration and deconfliction of threat information with other partners located within their jurisdiction and across their region, including HIDTAs, RISS Centers, DHS intelligence, operational, investigative, and analytic entities, FBI Field Offices, JTTFs, and major city/county intelligence units.

State and urban area fusion centers receiving SHSP or UASI grant funds will be evaluated based on compliance with the guidance and requirements for the National Network as set forth by DHS Intelligence and Analysis (I&A) through the annual Fusion Center Assessment.

- Additional fusion center grant requirements, including 28 C.F.R. Part 23 requirements, are listed at the Fusion Center Performance Program's HSGP page on DHS.gov and in the 28 C.F.R. Part 23 Online Training.

- FEMA approved analyst courses that meet the grant requirement are listed at FEMA Approved Intelligence Analyst Training Courses page on DHS.gov.

Through the PPR, fusion centers will report on the compliance with measurement requirements within the fusion centers through the annual Fusion Center Assessment managed by DHS I&A and reported to FEMA. In addition to the activities identified in the National Prevention Framework, fusion centers are also **required** to collaborate with those analytic, investigative, and information-sharing entities focused on preventing, detecting, deterring, and disrupting acts of terrorism and combating transnational criminal organizations. Such entities include, but are not limited to JTTFs, AMSC, Border Enforcement Security Task Forces, Integrated Border Enforcement Teams, HIDTAs, and RISS Centers, as well as other federal intelligence, operational, analytic, and investigative entities. **Applicants will be required to provide information regarding their information sharing partnerships, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing, via the Information and Intelligence National Priority Investment and supporting data via the annual Fusion Center Assessment**.

8.5.1. FUSION CENTER PERFORMANCE MEASURES

Table 7: Fusion Center Performance Measures

Reference Number*	Performance Measures
YEAR.1	Percentage of federal Information Intelligence Reports (IIRs) originating from fusion center information that address a specific Intelligence Community need

Reference Number*	Performance Measures
YEAR.2	Percentage of federal IIRs originating from fusion center information that the Intelligence Community otherwise used in performing its mission (e.g., contained first-time reporting; corroborated existing information; addressed a critical intelligence gap; or helped to define an issue or target)
YEAR.3	Number of SARs vetted and submitted by fusion centers that result in the initiation or enhancement of an investigation by the FBI
YEAR.4	Number of SAR vetted and submitted by fusion centers that involve an individual on the Watchlist
YEAR.5	Percentage of Requests for Information (RFIs) from the Terrorist Screening Center (TSC) for which fusion centers provided information for a TSC case file
YEAR.6	Percentage of I&A Watchlist nominations that were initiated or updated existing case files based on information provided by fusion centers
YEAR.7	Number of distributable analytic products co-authored by one or more fusion centers and/or federal agencies
YEAR.8	Percentage of fusion center distributable analytic products that address Homeland Security topics
YEAR.9	Percentage of fusion center distributable analytic products that address state/local customer information needs
YEAR.10	Percentage of key customers reporting that fusion center products are relevant
YEAR.11	Percentage of key customers reporting that fusion center services are relevant
YEAR.12	Percentage of key customers reporting that fusion center products are timely for mission needs
YEAR.13	Percentage of key customers reporting that fusion center services are timely for mission needs
YEAR.14	Percentage of key customers reporting that fusion center products influenced their decision making related to threat response activities within their AOR
YEAR.15	Percentage of key customers reporting that fusion center services influenced their decision making related to threat response activities within their AOR
YEAR.16	Percentage of key customers reporting that fusion center products resulted in increased situational awareness of threats within their AOR
YEAR.17	Percentage of key customers reporting that fusion center services resulted in increased situational awareness of threats within their AOR
YEAR.18	Number of tips and leads vetted by the fusion center
YEAR.19	Number of tips and leads vetted by the fusion center that were provided to other F/SLTT agencies for follow up action

Reference Number*	Performance Measures
YEAR.20	Number of responses to RFIs from all sources
YEAR.21	Number of situational awareness products developed and disseminated by fusion centers
YEAR.22	Number of case support and/or tactical products developed and disseminated by fusion centers
YEAR.23	Percentage of federally designated special events in which fusion centers played a direct role
YEAR.24	Percentage of federally declared disasters in which fusion centers played a direct role
YEAR.25	Number of public safety incidents in which fusion centers played a direct role

*"YEAR" should be changed for the current fiscal year, e.g., 2024, 2025, etc. Any updates to Performance Measures will be noted in the HSGP NOFO.

8.6. Investment Modifications – Changes in Scope or Objective (Tribal Homeland Security Grant Program)

Changes in scope or objective of the award—including those resulting from intended actions by the recipient or subrecipients—require FEMA's prior written approval, in accordance with 2 C.F.R. § 200.308(c)(1), § 200.407. THSGP is competitive with applications recommended for funding based on threat, vulnerability, and consequence, and their mitigation of potential terrorist attacks. However, consistent with 2 C.F.R § 200.308(c)(1), Change in Scope Prior Approval, FEMA requires prior approval of any change in scope or objective of the grant-funded activity after the award is issued. *See* 2 C.F.R. § 200.308(b), (c). Scope or objective changes will be considered on a case-by-case basis provided the change does not negatively impact the competitive process used to recommend THSGP awards.

Requests to change the scope or objective of the grant-funded activity after the award is made must be submitted via FEMA GO as a Scope Change Amendment. The amendment request must include the following:

- A written request on the recipient's letterhead outlining the scope or objective change including the approved projects from the IJ, the funds and relative scope or objective significance allocated to those projects, the proposed changes, and any resulting reallocations as a result of the change of scope or objective;
- An explanation why the change of scope or objective is necessary;
- How the proposed scope or objective changes to the project support the vulnerabilities and capability gaps identified in the approved IJ; and
- The request must also address whether the proposed changes will impact the recipient's ability to complete the project within the award's POP.

Recipients may not proceed with implementing any scope or objective changes until they receive prior written approval from FEMA through FEMA GO.

8.7. Continuity Capability (Homeland Security Grant Program, Tribal Homeland Security Grant Program)

Continuity should be integrated into each core capability and the coordinating structures that provide them. Continuity capabilities increase resilience and the probability that organizations can perform essential functions in the delivery of core capabilities that support the mission areas. FEMA is responsible for coordinating the implementation and development, execution, and assessment of continuity capabilities among executive departments and agencies. To support this role, FEMA develops and promulgates directives, policy, and guidance for federal and SLTT governments, non-governmental organizations, and private sector critical infrastructure owners and operators. Federal Continuity Directives (FCD) establish continuity program and planning requirements for executive departments and agencies, while FEMA's Continuity Guidance Circular (CGC) tailors' continuity guidance to SLTT and other non-Federal audiences. This direction and guidance assist in developing capabilities for continuing the essential functions of federal and SLTT governmental entities, as well as public/private critical infrastructure owners, operators, and regulators enabling them.

The FCDs, CGC, and the Continuity Resource Toolkit provide guidance and resources for organizations. For additional information on continuity programs, guidance, and directives, see the Continuity Resources and Technical Assistance page on FEMA.gov.

8.8. Senior Advisory Committee (Homeland Security Grant Program)

To support the whole community approach (see Section 1.6 "Strengthening Governance Integration" and Section 6.13 "Whole Community Preparedness"), the SAA must establish or reestablish a unified Senior Advisory Committee (SAC). The SAC builds upon previously established advisory bodies under SHSP, UASI, TSGP, and PSGP. Examples of advisory bodies that should be included on a SAC include Urban Area Working Groups (UAWGs), SIGB, AMSCs, Regional Transportation Security Working Groups (RTSWG), Citizen Corps Whole Community Councils, Disability Inclusion Working Groups, and Children's Working Groups. The membership of the SAC must reflect a state's unique risk profile and the interests of the five mission areas as outlined in the Goal. Further, the SAC must include representatives that were involved in the production of the state's THIRA and SPR.

8.8.1. SENIOR ADVISORY COMMITTEE COMPOSITION AND SCOPE

SAC membership shall include at least one representative from relevant stakeholders including:

- Individuals from the counties, cities, towns, and Tribal Nations within the state or high-risk urban area including, as appropriate, representatives of rural, high-population, and high-threat jurisdictions of UASI-funded high-risk urban areas;
- Representatives that were involved in the production of the state's THIRA and SPR;
- State and urban area Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs);
- SWIC and SIGB members;
- Citizen Corps Whole Community Councils;
- Local and tribal government officials;

- Tribal organizations and associations;
- Emergency response providers, including representatives of the fire service, law enforcement, emergency medical services, and emergency managers;
- Public health officials and other appropriate medical practitioners;
- Hospitals;
- Individuals representing educational institutions, including elementary schools, middle schools, junior high schools, high schools, community colleges, and other institutions of higher education;
- State and regional interoperable communications coordinators, as appropriate;
- State and major urban area fusion centers, as appropriate; and
- Nonprofit, faith-based, and other voluntary organizations, such as the American Red Cross.

Additionally, program representatives from the following entities should be members of the SAC (as applicable): State Primary Care Association, State Homeland Security Advisor (if this role is not also the SAA), State Emergency Management Agency (EMA) Director, State Public Health Officer, State Awardee for HHS' Hospital Preparedness Program, State Public Safety Officer (and SAA for Justice Assistance Grants, if different), State Coordinator for the DoD 1033 Program (also known as the Law Enforcement Support Office [LESO] Program), State Court Official, State Emergency Medical Services (EMS) Director, State Trauma System Manager, Statewide Interoperability Coordinator, State Citizen Corps Whole Community Council, the State Emergency Medical Services for Children (EMSC) Coordinator, State Education Department, State Human Services Department, State Child Welfare Services, State Juvenile Justice Services, Urban Area Points of Contact (POC), Senior Members of AMSCs, Senior Members of the RTSWG, Senior Security Officials from Major Transportation Systems, and the Adjutant General.

SACs are encouraged to develop subcommittee structures, as necessary, to address the issue or region-specific considerations. The SAC must include whole community intrastate and interstate partners as applicable and have balanced representation among entities with operational responsibilities for terrorism/disaster prevention, protection, mitigation, and response activities within the state, and include representation from the stakeholder groups and disciplines identified above.

The above membership requirement does not prohibit states, high-risk urban areas, regional transit and port entities, or other recipients of FEMA preparedness funding from retaining their existing structure under separate programs; however, at a minimum, those bodies must support and feed into the larger SAC. The composition, structure, and charter of the SAC should reflect this focus on building core capabilities, instead of simply joining previously existing advisory bodies under other grant programs. For designated high-risk urban areas, the SAA POCs are responsible for identifying and coordinating with the POC for the UAWG, which should be a member of the SAC. The POC's contact information must be provided to FEMA with the grant application. SAAs must work with existing high-risk urban areas to ensure that information for current POCs is on file with FEMA.

Finally, FEMA recommends that organizations advocating on behalf of youth, older adults, individuals with disabilities, and others with access and functional needs be invited to participate in the SAC. Applicants must submit the list of SAC members and the SAC charter at the time of application as an attachment in FEMA GO. SAAs will use the URT to verify compliance with SAC charter requirements.

8.8.2. SENIOR ADVISORY COMMITTEE RESPONSIBILITIES

The responsibilities of a SAC include:

- Integrating preparedness activities across disciplines, the private sector, nonprofit, faith-based, and community organizations, and SLTT governments, with the goal of maximizing coordination and reducing duplication of effort;
- Creating a cohesive planning network that builds and implements preparedness initiatives using FEMA resources as well as other federal, SLTT, private sector, and faith-based community resources;
- Managing all available preparedness funding sources to ensure their effective use and to minimize duplication of effort;
- Ensuring investments support building capability, closing capability gaps, or sustaining capabilities identified in the THIRA/SPR;
- Assisting in preparation and revision of the state, regional, or local homeland security plan or the THIRA, as the case may be; and
- Assisting in determining effective funding priorities for SHSP grants.

8.8.3. SENIOR ADVISORY COMMITTEE CHARTER

The governance of SHSP and UASI through the SAC should be directed by a charter. All members of the SAC should sign and date the charter showing their agreement with its content and their representation on the Committee. Revisions to the governing charter must be sent to the recipient's assigned FEMA HQ Preparedness Officer. The SAC charter must at a minimum address the following:

- A detailed description of the SAC's composition and an explanation of key governance processes, including how the SAC is informed by the states and urban area's THIRA/SPR;
- A description of the frequency at which the SAC will meet;
- How the committee will leverage existing governance bodies;
- A detailed description of how decisions on programmatic priorities funded by SHSP and UASI are made and how those decisions will be documented and shared with its members and other stakeholders, as appropriate; and
- A description of defined roles and responsibilities for financial decision making and meeting administrative requirements.

To ensure ongoing coordination efforts, SAAs are encouraged to share community preparedness information submitted in a state's BSIR with members of the SAC. SAAs are also encouraged to share their THIRA/SPR data with members of the SAC who are applying for other FEMA preparedness grants to enhance their understanding of statewide capability gaps. The charter should be made available upon request to promote transparency in decision-making related to SHSP and UASI activities.

To manage this effort and to further reinforce collaboration and coordination across the stakeholder community, a portion of the 20% holdback of a state or territory award may be utilized by the SAA to support the SAC and to ensure representation and active participation of SAC members. Funding may be used for hiring and training planners, establishing and maintaining a program management structure, identifying and managing projects, conducting research necessary to inform the planning process, and developing plans that bridge mechanisms, documents, protocols, and procedures.

8.9. Urban Area Working Group (Homeland Security Grant Program)

To support the whole community approach (see Section 1.6 "Strengthening Governance Integration" and Section 6.13 "Whole Community Preparedness"), high-risk urban areas are required to establish UAWGs representative of the counties, cities, towns, and Tribal Nations within the high-risk urban area including, as appropriate, representatives of rural jurisdictions, high-population jurisdictions, and high-threat jurisdictions.

UASI implementation and governance must include regional partners and should have balanced representation among entities with operational responsibilities for prevention, protection, mitigation, and response activities within the region. In some instances, high-risk urban area boundaries cross state borders. States and territories must ensure that the identified high-risk urban areas take an inclusive regional approach to the development and implementation of the UASI and involve the contiguous jurisdictions, mutual aid partners, port authorities, rail and transit authorities, state agencies, Statewide Interoperability Coordinators, Citizen Corps Whole Community Council(s), and campus law enforcement in their program activities.

8.9.1. URBAN AREA WORKING GROUP COMPOSITION AND SCOPE

Pursuant to section 2003(b) of the HSA (codified as amended at 6 U.S.C. § 604(b)), eligible high-risk urban areas were determined based on an analysis of relative risk of the 100 most populous Metropolitan Statistical Areas (MSA), as defined by OMB. MSAs are used by FEMA to determine eligibility for participation in the program. Geographical areas queried do not equate to minimum mandated membership representation of an urban area, nor does this guarantee funding for geographical areas queried. UAWGs are not required to expand or contract existing urban area participation to conform to MSA composition. Detailed information on MSAs is publicly available from the United States Census Bureau.

An SAA must confirm a specific POC with the designated high-risk urban area. The SAA POC is responsible for identifying and coordinating with the POC for the UAWG. This information must be provided to FEMA with the grant application. SAAs must work with existing high-risk urban areas to ensure that information for current POCs is on file with FEMA.

Membership in the UAWG must provide either direct or indirect representation for all relevant jurisdictions and response disciplines (including law enforcement, fire service, EMS, hospitals, public health, and emergency management) that comprise the defined high-risk urban area. It must also be inclusive of local Citizen Corps Whole Community Council and tribal representatives. The UAWG should also include at least one representative from each of the following significant stakeholders:

- Local and tribal government officials;
- CIO and CISO;

- Emergency response providers, which shall include representatives of the fire service, law enforcement, emergency medical services, and emergency managers;
- Public health officials and other appropriate medical practitioners, including Health Care Coalitions (HCCs);
- Individuals representing educational institutions, including elementary schools, middle schools, junior high schools, high schools, community colleges, and other institutions of higher education; and
- State and regional interoperable communications coordinators and state and major urban area fusion centers, as appropriate.

In addition to representatives from the local jurisdictions and Tribal Nations within the state, territory, or high-risk urban area, the UAWG should include officials responsible for the administration of Centers for Disease Control and Prevention's (CDC) and the HHS Assistant Secretary for Preparedness and Response's (ASPR) cooperative agreements. Finally, it must include members advocating on behalf of youth, older adults, individuals with disabilities, and others with- access and functional needs.

High-risk urban areas will use the URT to verify UAWG structure and membership. The list of UAWG members must also be submitted at the time of application as an attachment in FEMA GO. High-risk urban areas must notify the SAA and the FEMA Headquarters Preparedness Officer of any updates to the UAWG structure or membership after the application is submitted.

8.9.2. URBAN AREA WORKING GROUP RESPONSIBILITIES

UAWGs must ensure that applications for funding under the UASI support building capability, closing capability gaps, or sustaining capabilities identified in the high-risk urban area's THIRA/SPR. The UAWG should support state efforts to develop the SPR particularly as it relates to UASI-funded activities. The UAWG, in coordination with the SAA POC, must develop a methodology for allocating funding available through the UASI. The UAWG must reach consensus on all UASI funding allocations. If consensus cannot be reached within the 45-day period allotted for the state to obligate funds to subrecipients, the SAA must make the allocation determination. The SAA must provide written documentation verifying the consensus of the UAWG or the failure to achieve otherwise on the allocation of funds and submit it to FEMA immediately after the 45-day period allotted for the state to obligate funds to subrecipients. Any UASI funds retained by the state must be used in direct support of the high-risk urban area. States must provide documentation to the UAWG, and FEMA upon request, demonstrating how any UASI funds retained by a state are directly supporting the high-risk urban area.

8.9.3. URBAN AREA WORKING GROUP CHARTER

In keeping with sound project management practices, the UAWG must ensure that its approach to critical issues such as membership, governance structure, voting rights, grant M&A responsibilities, and funding allocation methodologies are formalized in a working group charter, or another form of standard operating procedure related to the UASI governance. The charter must also outline how decisions made in UAWG meetings will be documented and shared with UAWG members. The UAWG charter must be submitted at the time of application as an attachment in FEMA GO and must be on file with FEMA prior to drawing down UASI funding. It also must be available to all UAWG members to promote transparency in decision making related to the UASI.

8.10. Supplemental State Homeland Security Program and Urban Area Security Initiative Guidance (Homeland Security Grant Program)

8.10.1. COLLABORATION WITH OTHER FEDERAL PREPAREDNESS PROGRAMS

FEMA strongly encourages states, high-risk urban areas, Tribal Nations, and territories to understand other federal preparedness programs in their jurisdictions and to work with them in a collaborative manner to leverage all available resources and avoid duplicative activities. For example, HHS has two robust preparedness programs—CDC's Public Health Emergency Preparedness (PHEP) cooperative agreement and ASPR's Hospital Preparedness Program (HPP) cooperative agreement—that focus on preparedness capabilities. CDC's 15 public health preparedness capabilities and ASPR's 4 healthcare preparedness capabilities serve as operational components for many of the core capabilities, and collaboration with the PHEP directors and HPP coordinators can build capacity around shared interests and investments that fall in the scope of these HHS cooperative agreements and the HSGP.

States and high-risk urban areas should coordinate among the entire scope of federal partners, national initiatives, and grant programs to identify opportunities to leverage resources when implementing their preparedness programs. These may include but are not limited to: Medical Reserve Corps; Emergency Medical Services for Children grants; ASPR HPP; CDC PHEP; CDC Cities Readiness Initiative; Strategic National Stockpile Programs; EMS; DOJ grants; the Department of Defense 1033 Program (also known as the LESO Program); and CISA's Infrastructure Security Division. However, coordination is not limited to grant funding. It also includes leveraging assessments such as the Transportation Security Administration's (TSA) Baseline Assessment for Security Enhancement (BASE), reporting from the Intelligence Community, risk information such as USCG's Maritime Security Risk Analysis Model (MSRAM), and USBP Sector Analysis.

Each SHSP- and UASI-funded investment that addresses biological risk, patient care, or health systems preparedness should be implemented in a coordinated manner with other federal programs that support biological and public health incident preparedness such as those administered by HHS ASPR, CDC, and DOT's National Highway Traffic Safety Administration (NHTSA).

8.10.2. COLLABORATION WITH HEALTH CARE COALITIONS

Health Care Coalitions (HCC) are regional entities comprised of health care, public health, emergency management, and emergency medical services organizations that plan and respond together, leverage resources, and address challenges in health care delivery brought on by public health and medical incidents. Given that many of the risks being mitigated include the potential for a range of mass casualties, including those across the chemical, biological, radiological, nuclear, explosive (CBRNE) spectrum, planning efforts should include the participation of HCCs and should take into account the elements and capabilities articulated in the Health Care Preparedness and Response Capabilities for Health Care Coalitions, and other forthcoming versions.

8.10.3. COLLABORATION WITH NONPROFIT ORGANIZATIONS

SHSP and UASI recipients are encouraged to work with the nonprofit community to address terrorism and all-hazards prevention concerns, seek input on the needs of the nonprofit sector, and support the goals of their investments.

8.10.4. COLLABORATION WITH TRIBAL NATIONS

Tribal governments and their members are an essential part of our nation's emergency management team. Effective relationships with Tribal Nations are necessary to fulfill FEMA's mission of working together to improve our nation's preparedness and response posture. As such, FEMA strongly encourages states, high-risk urban areas, and territories to work with Tribal Nations in overall initiatives, such as whole community preparedness and emergency management planning.

8.11. Operation Stonegarden Operational Guidance (Homeland Security Grant Program)

This section provides OPSG operational guidance on campaign planning, the tactical operation period, and reporting procedures. This guidance also delineates specific roles and responsibilities, expectations for operations, and performance measures. Successful execution of these objectives will promote situational awareness among participating agencies and ensure a rapid, fluid response to emerging border security conditions.

OPSG uses an integrated approach to address transnational criminal activity. Federal and SLTT partners are required to establish and maintain an OPSG Integrated Planning Team (IPT) with representation from all participating law enforcement agencies and co-chaired by representatives from USBP, the SAA, and participating local law enforcement agencies' OPSG program representatives. Each operational order will address specific threats, gaps, and vulnerabilities identified by the USBP. All requests in the operational plan will be reviewed and approved by the corresponding sector's Chief Patrol Agent or his/her designee for border security value. USBP will provide routine monitoring and technical expertise to each participating agency. The content of each operational plan, to include the requested items, will be reviewed for border security value and approved by the corresponding sector's Chief Patrol Agent or his/her designee.

All operational plans should be crafted in cooperation and coordination with federal and SLTT partners to meet the needs of the USBP Sector. Consideration will be given to applications that are coordinated across multiple jurisdictions. All applicants must coordinate with the CBP/USBP Sector Headquarters with geographic responsibility for the applicant's location in developing and submitting an Operations Order with an embedded budget to the SAA. Operations are to be crafted so that resources are allocated to one or more of the supportable categories:

1. Law Enforcement Presence;
2. Situational Awareness; and/or
3. Intelligence Collection, Analysis, and Distribution.

Law Enforcement Presence includes activities and costs associated to having an SLTT partner provide a law enforcement patrol presence in an area designated by the USBP Sector in support of border security efforts. Situational Awareness includes technology to provide current and immediately relevant information about currently active border security threats. Intelligence Collection, Analysis, and Distribution includes both technology and manpower related to the gathering and analysis of intelligence with a nexus to border security.

The terms of an OPSG award do not extend to an SLTT partner any authority to enforce additional laws, statutes, or regulations beyond their own authorities; SLTT partners are not empowered through OPSG to enforce immigration authorities under Title 8 of the U.S. Code (i.e., the Immigration and Nationality Act [INA]). Participation in the grant does not grant participants the power to operate outside of their own jurisdictional boundaries.

8.11.1. CAMPAIGN PLANNING

Campaign Plan

After awards are announced, participants will create and submit an operations order that forms a campaign plan and captures the initial, generalized-budgetary intent to their IPT.

The campaign plan should articulate the participant agency's long-term border security objectives and goals designed to mitigate border security risk.

Funds should be obligated as needed to target specific threats or vulnerabilities and ensure that OPSG usage is commensurate to the unique risk of each border region. This may require several short-term operations that combine to form an ongoing operational cycle, ensuring that USBP commanders and SLTT agency partners reserve the flexibility to respond to the ever-changing elements of border security.

The operations plan also will articulate the budgetary intent of how funds are to be used throughout the performance period. The operations plan will project planned expenditures in the following categories: overtime, equipment, travel, maintenance, fuel, and administrative funds. The subrecipient can initiate the procurement of equipment as well as state how much the county intends to use for M&A while keeping funds for overtime or residual equipment funds available for use as needed. If the subrecipient intends to spend more than 50% of its award on overtime over the course of the performance period, a Personal Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act (PRICE Act) waiver request must be submitted following the process described in the HSGP NOFO. The operations plan will meet both the SAA expectations to obligate the funds within 45 days of the award announcement and the demands of the grant's operational intent. **Sector approved campaign plans must be submitted to USBP Headquarters no later than four months after the official awards announcement has been made.**

Investment Modifications - Changes in Scope or Objective

Changes in scope or objective of the award – including those resulting from intended actions by the recipient or subrecipients – require FEMA's prior written approval, in accordance with 2 C.F.R. § 200.308(c)(1), § 200.407.

If changes must be made to the original operational plan, such as additional funding requests or other changes to the original scope or objectives, a FRAGO must be submitted in Homeland Security Information Network (HSIN) to obtain FEMA's prior written approval of such changes in accordance with 2 C.F.R. § 200.308(c)(1). These modifications will be annotated in the annex section of the FRAGO.

Operational Execution

If changes or additional funding requests to the original operational order must be made, a FRAGO will be created. These modifications will be annotated in the annex section of the FRAGO. Operational discipline is necessary for the success of OPSG. Deliberate, adaptive, integrated, and intelligence-driven planning is critical to conducting targeted enforcement operations consistent with the objectives of the OPSG. By participating in the OPSG, the SLTT agencies agree to conduct operations designed to reduce border security risk.

Operations are composed of six critical elements: 1) a pre-planning meeting with the IPT; 2) specified beginning and ending dates; 3) the integration of intelligence and border security; 4) use of targeted

enforcement techniques; 5) clearly stated objectives; and 6) an after-action meeting. These operations require deliberate on-going planning to ensure command, staff, and unit activities synchronize to current and future operations. The cyclical nature of the process will ensure OPSG activities align with the fluctuating border security threats and vulnerabilities. The IPT should leverage information provided by the fusion center, Border Intelligence Centers, or other local intelligence center when possible and establish a common operational vision.

The USBP Sector's Chief Patrol Agent or his/her designee will ensure that the information or intelligence has a clear nexus to border security. Intelligence will be shared and vetted for border security value, driving the focus of operations. Once intelligence-driven targets are identified, the IPT will decide on operational objectives that reflect the intended impact of operations. The objectives should outline how the operation will deter, deny, degrade, or dismantle the operational capacity of the targeted transnational criminal organizations.

Each operational period will begin on a predetermined date and end on a predetermined date; however, dates may be subject to change commensurate with emerging security conditions. The starting date of the operational period should be established to allow sufficient time for the order to be submitted and approved by the corresponding USBP Sector and in concurrence with its SAA and USBP Headquarters. The USBP Sectors will upload copies of the operations order in the corresponding folder in the CBP Stonegarden Data Management System.

8.11.2. REPORTING PROCEDURES

Participation in OPSG requires accurate, consistent, and timely reporting of how funds are used, and how the SLTT agencies' operations have impacted border security through the mitigation of threat or vulnerability and the overall reduction of risk. Reporting will focus on monitoring program performance; determining the level of integration and information sharing; and developing best practices for future operations. To ensure consistent reporting each SLTT agency will identify a single point of contact to represent their agency as a member of the IPT and to coordinate the submission of reports or execute other aspects of the grant.

The Daily Activity Report (DAR), which can be found by selecting the current fiscal year HSGP NOFO on FEMA's preparedness grants page, is to be used to submit the ongoing results and outputs from OPSG operations conducted. The information and statistics included in the DAR will be delineated by agency (friendly forces). The DAR must be submitted to the USBP sector or the participating agency's OPSG coordinator within 48 hours of the conclusion of each OPSG shift. Subrecipients and Sectors are responsible to ensure that DARs are submitted in the proper format and in a timely manner. DARs will be submitted using the CBP Stonegarden Data Management System. Friendly forces receiving funding through a subrecipient will submit DARs within 48 hours. Border Patrol Sectors and OPSG subrecipients will implement internal protocols to ensure operational data from subrecipients and friendly force DARs are properly collected following the established guidelines.

In addition to the ongoing reporting of outputs, subrecipient participants will be required to submit AARs to USBP sectors within 10 days of closing the operational POP for that funding year. The AAR should carefully articulate outcomes and outputs as well as how the results of the operation compare with the objectives identified during the pre-planning meeting. Failure to submit the AAR in a timely manner may prevent the approval of future operations requests. All AARs and other OPSG reporting requirements will be submitted through the CBP Stonegarden Data Management System. Sectors are responsible for submitting AARs into Border Patrol Enforcement Tracking System (BPETS) as applicable.

8.11.3. OPERATION STONEGARDEN COORDINATION

OPSG supports enhanced cooperation and coordination among CBP, USBP, and federal and SLTT law enforcement agencies to improve overall border security. OPSG provides funding to support joint efforts to secure the United States' borders along routes of ingress/egress of international borders including travel corridors in states bordering Mexico and Canada along with states and territories with international water borders. OPSG also further enhances the sharing of threat information and intelligence between federal and SLTT law enforcement agencies through the development and sustainment of a capable workforce of analysts that have the necessary experience and training, access to open source, unclassified and classified information, products, data, SAR, tips/leads, and online/social media-based threats as well as necessary services and technology to facilitate analytic capabilities and collaboration.

SLTT law enforcement agencies will utilize their own law enforcement authorities to support the CBP and USBP border security mission and will not receive any additional authority as a result of participation in the grant. An OPSG award does not provide any additional authority to SLTT law enforcement agencies. More specifically, SLTT law enforcement agencies are not empowered through OPSG to enforce immigration authorities under Title 8 of the U.S. Code (i.e., the INA).

SLTT law enforcement agencies are expected utilize their own jurisdictional authority in support of enhanced border security unless some other agreement applies. SLTT law enforcement agencies are further expected to operate within the bounds of all applicable laws, to include federal laws, state statutes, and local laws, policies, and procedures.

OPSG is intended to support border states and territories of the United States in accomplishing the following objectives:

- Increase intelligence and operational capabilities to prevent, protect against, and respond to border security issues;
- Increase coordination and collaboration among federal and SLTT law enforcement agencies;
- Continue the distinct capability enhancements required for border security and border protection;
- Provide intelligence-based operations through USBP Sector Level experts to ensure safety and operational oversight of federal and SLTT law enforcement agencies participating in OPSG operational activities;
- Support a request to any Governor to activate, deploy, or redeploy specialized National Guard Units/Packages and/or elements of state law enforcement to increase or augment specialized/technical law enforcement elements operational activities;
- Continue to increase operational, material, and technological readiness of SLTT law enforcement agencies;
- Enhance the sharing of threat information and intelligence between federal and SLTT law enforcement agencies; and
- Develop and sustain a capable workforce of analysts that have the necessary experience and training, as well as access to open source, unclassified and/or classified information, products,

data, SAR, tips/leads, online/social media-based threats, and the necessary services and technology to facilitate these analytic activities.

OPSG funds must be used to provide an enhanced law enforcement presence and to increase operational and intelligence capabilities of federal and SLTT law enforcement, promoting a layered, coordinated approach to law enforcement within border states and territories of the United States.

- **Federal and SLTT OPSG IPT:** Federal and SLTT partners must establish and maintain a formalized OPSG IPT with representation from all participating law enforcement agencies, co-chaired by representatives from USBP, the SAA, and participating law enforcement agencies' OPSG program representatives.
- **One IPT meeting must take place during every funding year** before submitting the Campaign Plan
- OPSG funds may be used for travel and per diem in support of the IPTs and OPSG strategic planning events if the costs are otherwise compliant with other program and regulatory requirements.

8.11.4. COORDINATION REQUIREMENTS

All operational plans should be crafted in cooperation and coordination among federal and SLTT partners. Consideration will be given to applications that are coordinated across multiple jurisdictions. All applicants must coordinate with the USBP Sector Headquarters with geographic responsibility for the applicant's location in developing and submitting an Operations Order with an embedded budget to the SAA. OPSG funds must be used to provide increased operational capabilities to SLTT partners in support of enhanced border security through:

- Enhanced Law Enforcement Presence;
- Enhanced Situational Awareness; and
- Enhanced Intelligence Collection and Distribution.

After awards are announced, prospective recipients will re-scope the draft Operations Order and resubmit it as a final Operations Order with an embedded budget based on actual dollar amounts awarded. The appropriate Sector Headquarters will approve final Operations Orders and forward those orders to Headquarters, Office of Border Patrol, Washington, D.C., before funding is released. Recipients may not begin operations, obligate, or expend any funds until FEMA and USBP Headquarters have approved the final Operations Order and the embedded budget and removed any existing special conditions and/or restrictions.

8.11.5. OPERATIONAL ROLES AND RESPONSIBILITIES

To achieve unity of effort, it is essential that each participant know the roles and responsibilities within the IPT. The USBP sector's Chief Patrol Agent, or his/her designee, will:

- Coordinate and chair the area IPT's meetings;
- Coordinate with all interested and eligible SLTT agencies in the sector's area of operation during the open period of the OPSG application process by:

  - Assisting applicants in completing the operations planning portion of the application, which is like the Operations Order used by the USBP;
  - Forwarding the approved operation portion of the application to CBP/USBP Headquarters as well as to the SAA to complete the application process set by FEMA; and
  - Detailing what operational support the USBP Sector anticipates for specific periods and matching the capabilities of partners to fill those gaps.

- Following the announcement of grant awards, coordinate and chair a meeting with SLTT agencies that received OPSG awards to develop an individualized campaign plan. This includes:
  - Working with SLTT agencies along with other federal law enforcement agencies to determine the dates, focus, and needs of each operational period thus ensuring that each operation has a nexus to border security;
  - Receiving the first periodic operations order from the SLTT agencies and ensuring that the operation is conducted as outlined in the Campaign Planning section;
  - Monitoring and supporting the Operational Cycle throughout the performance period;
  - Ensuring the DAR and the AAR are submitted by SLTT agencies in the proper format and within the established timeframes;
  - Providing instruction, when possible, to SLTT agencies regarding techniques, methods, and trends used by transnational criminal organizations in the area;
  - Providing a single point of contact to participants as a subject-matter expert in OPSG that can coordinate, collect, and report operational activities within the established reporting procedures;
  - Providing verification that operations are conducted;
  - Documenting and conducting random, on-site operational verification of OPSG patrols by subrecipients and friendly forces;
  - Verifying that subrecipients are performing OPSG enforcement duties in accordance with the applicable grant, statute, and regulatory guidance and instructions; and
  - Ensuring that grant funds are appropriately expended to meet sector border enforcement operational requirements and assist in enhancing subrecipient/friendly force capabilities to provide for enhanced enforcement presence, operational integration, and intelligence sharing in border communities.

The SLTT agency lead, or their designee, will:

- Coordinate with the SAA on all grant management matters including but not limited to the development and review of operations orders, expenditure of funds, allowable costs, reporting requirements;
- Upon receiving a grant award, coordinate and meet as a member of the IPT to develop an individualized campaign plan that covers the length of the grant performance period;

- Work within the IPT to develop an initial Operational Cycle and determine the duration of the first operational period based on the tactical needs specific to the area;
- Submit all operations orders for review and submit the operations order to the Border Patrol and ensure the operation meets the six criteria established in the Operational Execution Section (see Section 8.11.1 "Campaign Planning"):
    - Conduct operations as needed throughout the length of the grant performance period;
    - Integrate law enforcement partners from contiguous counties and towns into their tactical operations to expand the layer of security beyond existing areas;
    - Ensure all required reports, including reports from friendly forces, are submitted to the Border Patrol and the SAA, when applicable, in the proper format and within established timeframes;
    - Ensure applicable OPSG-derived data is shared with the designated fusion center in the state or high-risk urban areas;
    - Ensure applicable intelligence is shared with the designated fusion center in the state and/or high-risk urban areas;
    - Request instruction and information from the SAA, when applicable, and/or USBP and other federal law enforcement agencies regarding techniques, methods, and trends used by transnational criminal organizations in the area;
- Provide the SAA and USBP a single point of contact that maintains subject-matter expertise in OPSG who can coordinate, collect, and report operational activities within the established reporting procedures; and
- Assist as required with the coordination, management, and operational aspects of the grant.

The SAA will:

- Actively engage in the IPT meetings;
- Work in direct coordination and communication with the local or tribal agency lead on all grant management matters;
- Review all operations orders created by the local or tribal agency;
- Act as the fiduciary agent for the program and provide expertise in state policy and regulations;
- Enter into a subaward agreement to disburse the allocated funding awarded through FEMA;
- Generate biannual reports to FEMA capturing the subrecipients' obligations and expenditures of funds;
- Determine if the grant's performance period requires additional refinement over the federally established 36-month period;

- Conduct audits of the program to ensure that the subrecipients are following program guidance; and
- Assist as required with the coordination, management, and operational aspects of the grant.

8.11.6. DEFINITIONS (OPERATION STONEGARDEN)

Area of Interest: A specific area, areas, or facilities known to be used by transnational criminal organizations in furtherance of their criminal activity.

Border security related crime: Any action or enterprise that constitutes an offense which is punishable by law, for which prosecution would serve established border security goals as outlines by the CBP for a whole of community approach:

- That results in a favorable environment for criminal enterprise network, transnational criminal, or terrorist organizations; the smuggling/trafficking of humans, contraband, narcotics, or weapons of mass destruction across or in proximity to the U.S. border; or
- That has a direct nexus to illicit cross-border activity.

Campaign Plan: The first Operational Order aimed at accomplishing a strategic or operational objective within a given time and space.

FRAGO: A fragmentary order is a modification of the approved campaign plan, reflecting changes to the scope or objective pursuant to 2 C.F.R. § 200.308(c)(1). After an operation order has been approved, any changes to a campaign plan will be submitted via HSIN as a FRAGO for FEMA's approval. Subsequent FRAGOs are permissible, subject to FEMA's prior written approval, consistent with the requirements of 2 C.F.R. § 200.308, § 200.407.

Friendly Forces: Local law enforcement entities supporting border security operations to whom OPSG subrecipients provide funding.

IPT: Group that coordinates on all aspects of OPSG application, planning, and de-briefings.

Operational Cycle: A deliberate on-going cycle of command, staff, and unit activities intended to synchronize current and future operations (driven by current intelligence and short-term goals that support the campaign).

Operational Discipline: The organized manner in which an organization plans, coordinates, and executes the OPSG mission with common objectives toward a particular outcome.

Operation/Operational Order: A formal description of the action to be taken to accomplish or satisfy Campaign Plan or FRAGO. The Operation/Operational Order includes a detailed description of actions to be taken and required logistical needs to execute an operation.

Opioid Receptor Antagonists: Any medically approved drug or medical substance that can be used by first responder personnel in an emergency that is designed to counteract the effects of an opioid overdose.

Performance Measure: A numerical expression that quantitatively conveys how well the organization is doing against an associated performance goal, objective, or standard.

Risk: Potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.

Targeted Enforcement: The leveraging of all available assets against a specific action, area, individual, or organization and using those deemed most appropriate to mitigate risk.

Target of Interest: A specific person, group of persons, or conveyance known to be part of, or used by transnational criminal organizations to advance their criminal activity.

Threat: Information expressing intent to conduct illegal activity often derived from intelligence sources, the overall context, a specific event or series of events, or observation of suspicious activity.

Tier: Tier refers to the geographical location of a municipality, county, or Tribal Nation with respect to the United States national border, i.e., Tier 1 is a county located on the border; a Tier 2 county is a county contiguous to a Tier 1 county; and a Tier 3 is a county not located on the physical border but is a contiguous to a Tier 2 county.

Unity of Effort: Coordination and cooperation among all organizational elements, even though they may not be part of the same command structure, to achieve success.

Vulnerability: The protective measures in place are less than the protective measures needed to mitigate risk.

8.12. Pass-Through Requirements (Homeland Security Grant Program)

Awards made to the SAA for HSGP carry additional **statutorily mandated** pass-through requirements. Pass-through is defined as an obligation on the part of the SAA to make funds available to local units of government, combinations of local units, tribal governments, or other specific groups or organizations. These entities are defined at 6 U.S.C. § 101(13) as:

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government.
- An Indian Tribal Nation or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation.
- A rural community, unincorporated town or village, or other public entity.

Four criteria must be met to pass-through grant funds:

- The SAA must make a firm written commitment to passing through grant funds to subrecipients;
- The SAA's commitment must be unconditional (i.e., no contingencies for the availability of SAA funds);
- There must be documentary evidence (i.e., award document, terms, and conditions) of the commitment; and
- The award terms must be communicated to the subrecipient.

8.12.1. TIMING AND AMOUNT

The SAA must pass-through at least 80% of the funds awarded under SHSP and UASI to the above-defined local or tribal units of government within 45 calendar days of receipt of the funds. "Receipt

of the funds" occurs either when the SAA accepts the award or 15 calendar days after the SAA receives notice of the award, whichever is earlier.

SAAs are sent notification of HSGP awards via the FEMA GO system. If an SAA accepts its award within 15 calendar days of receiving notice of the award in the FEMA GO system, the 45 calendar days pass-through period will start on the date the SAA accepted the award. Should an SAA not accept the HSGP award within 15 calendar days of receiving notice of the award in the FEMA GO system, the 45 calendar days pass-through period will begin 15 calendar days after the award notification is sent to the SAA via the FEMA GO system.

It is important to note that the POP start date does not directly affect the start of the 45 calendar days pass-through period. For example, an SAA may receive notice of the HSGP award on August 25, while the POP starts on September 1. In this example, the 45-day pass-through period will begin on the date the SAA accepts the HSGP award or September 9 (15 calendar days after the SAA was notified of the award), whichever date occurs first. The POP start date of September 1 would not affect the timing of meeting the 45-calendar day pass-through requirement.

8.12.2. OTHER SHSP AND UASI PASS-THROUGH REQUIREMENTS

The signatory authority of the SAA must certify in writing to DHS/FEMA that pass-through requirements have been met. ***A letter of intent (or equivalent) to distribute funds is not considered sufficient*** and is not a firm commitment. and If a letter of intent is issued before FEMA makes the award, then the letter is also not unconditional since it is inherently conditioned on receipt of funds.

The pass-through requirement does not apply to SHSP awards made to the District of Columbia, Guam, American Samoa, the U.S. Virgin Islands, or the Commonwealth of the Northern Mariana Islands. ***The Commonwealth of Puerto Rico is required to comply with the pass-through requirement***, and its SAA must also obligate at least 80% of the funds to local units of government within 45 calendar days of receipt of the funds.

Under SHSP, the SAA may retain no more than 20% of funding for expenditures made by the state on behalf of the local unit(s) of government, such as expenditures by the state in order to pass through goods or services to local unit(s) of government in lieu of cash. This may occur only with the written consent, such as a Memorandum of Understanding, between the SAA and the local unit(s) of government. Separate written consent is necessary for each local unit of government in which no more than 20% of funding is retained on their behalf by the state. The written consent must specify the amount of funds to be retained and the intended use of funds, including whether any goods or services will be passed through in lieu of cash. It must also be signed by authorized representatives of both the state and the local unit of government.

States shall review their written consent agreements yearly and ensure that they are still valid. If a written consent agreement is already in place from previous FYs, DHS/FEMA will continue to recognize it for the current FY, unless the written consent review indicates the local government is no longer in agreement. If modifications to the existing agreement are necessary, the SAA should contact their assigned FEMA HQ Preparedness Officer. However, even if a written consent agreement is in place from previous FYs, ***the SAA must still initially carry out the pass-through documentation for its current FY award and comply with the four pass-through criteria described above before the written consent agreement can take effect for purposes of the current FY's funding.***
Under UASI, the SAA must obligate at least 80% of the grant funds to the high-risk urban area within 45 calendar days of receipt of the funds. Any funds retained (up to 20% of the award) by the SAA must be expended on items, services, or activities that benefit the high-risk urban area. The SAA

must provide each high-risk urban area with an accounting of the items, services, or activities provided to the urban area using the retained funds.

8.12.3. OPSG PASS-THROUGH REQUIREMENTS

Recipients cannot use or commit funds from OPSG until DHS/FEMA reviews and approves each specific county-level Operations Order or Fragmentary Operations Order budget. Approval will be communicated through an official email from DHS/FEMA lifting this special condition.

Under OPSG, SAAs must pass-through at least 97.5% of the awarded OPSG funds to county-level OPSG subrecipients. SAAs may retain up to 2.5% of the OPSG award amount for M&A costs associated with administering the awards.

8.13. Supplemental Resources (Homeland Security Grant Program, Tribal Homeland Security Grant Program)

FEMA collaborates with various subject-matter experts and acknowledges the value and expertise these Federal partner agencies provide to help shape the development and implementation of the HSGP and THSGP. This continued partnership and collaboration helps provide recipients with the greatest number of resources required to effectively manage and implement funds as well as promotes transparency. Therefore, FEMA is providing links to information on various subjects and policies that are relevant to the mission and intent of FEMA and its preparedness grant programs.

8.13.1. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DETECTION

The Countering Weapons of Mass Destruction (CWMD) Office is a support component within DHS established in December 2017 to counter attempts by terrorists or other threat actors to carry out an attack against the United States or its interests using a weapon of mass destruction. The CWMD Office provides guidance to improve national coordination on CBRN issues and works with federal and SLTT agencies to ensure operators have better access to current data and subject-matter expertise they need. FEMA offers implementation support on the THIRA/SPR for SLTT partners and the CWMD Office offers TA to provide guidance to SLTT partners seeking to address CBRN threats and to build or sustain CBRN detection and response capabilities. For more information or assistance, please contact CWMD-THIRA@hq.dhs.gov.

8.13.2. NATIONAL INFORMATION EXCHANGE MODEL

National Information Exchange Model (NIEM) is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM can save time and money by providing consistent, reusable data terms and definitions and repeatable processes. To support information sharing, all recipients of grants for projects implementing information exchange capabilities are required to use NIEM and to adhere to the NIEM compliance rules. Go to NIEM.gov for guidance on how to utilize FEMA award funding for information sharing, exchange, and interoperability activities.

The NIEM Emergency Management domain supports emergency-related services (including preparing first responders and responding to disasters), information sharing, and activities such as homeland security and resource and communications management. The NIEM Emergency Management domain has an inclusive governance structure that includes federal, SLTT, industry, and, where necessary, international partnerships. The NIEM Emergency Management domain is committed to community support via TA and NIEM training. For more information on the NIEM

Emergency Management domain, to request training or TA or to just get involved, go to the Emergency Management page on NIEM.gov.

8.13.3. INFRASTRUCTURE RESILIENCE PLANNING FRAMEWORK

SLTT governments are faced with complex long-term decisions, limited sources of revenue, and changing populations. CISA developed the Infrastructure Resilience Planning Framework (IRPF) as a resource for SLTT planners. The IRPF provides a process and a series of tools and resources for incorporating critical infrastructure resilience considerations into planning activities. The IRPF can be used to support capital improvement plans, hazard mitigation plans, or other planning documents, as well as funding requests. For more information, see the IRPF. For more information on CISA's resiliency planning programs, see the CISA Resiliency Planning Program site.

8.13.4. REGIONAL RESILIENCY ASSESSMENT PROGRAM

The Regional Resiliency Assessment Program (RRAP) is a cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure that address a range of infrastructure resilience issues that could have regionally and nationally significant consequences. These voluntary, non-regulatory RRAP projects are led by CISA's Infrastructure Security Division and are selected each year by DHS with input and guidance from federal, state, and local partners. For additional information on the RRAP, visit the RRAP page on CISA.gov.

8.13.5. INTEGRATED PUBLIC ALERT AND WARNING SYSTEM

The Integrated Public Alert & Warning System (IPAWS) is FEMA's national system for local alerting that provides authenticated emergency and life-saving information to the public through mobile phones using Wireless Emergency Alerts, to radio and television via the Emergency Alert System, and on the National Oceanic and Atmospheric Administration's Weather Radio. For more information, see the IPAWS page on FEMA.gov.

8.13.6. HOMELAND SECURITY INFORMATION NETWORK

HSIN is a user-driven, web-based, information sharing platform that connects all homeland security professionals including the DHS and its federal, SLTT, international, and private sector partners across all homeland security mission areas. HSIN is used to support daily operations, events, exercises, natural disasters, and incidents. To support user mission needs, HSIN provides three sets of services for secure information sharing. The first service provides a shared place for communities to securely collaborate on homeland security issues and includes core functions such as a web conferencing and instant messaging tools with white boarding, video, and chat services for real-time communication and situational awareness. The second set provides secure dissemination and sharing capabilities for homeland security alerts, reports, and products. The third set allows users to access and query a variety of shared data and services from all homeland security mission areas and trusted federal partners. Preparedness grant funds may be used to support planning, training and development costs associated with developing and managing mission critical HSIN communities of interest and sites. Learn more about HSIN on the HSIN HSGP Guidance page on DHS.gov.

8.13.7. STATE, LOCAL, TRIBAL, TERRITORIAL CYBERSECURITY ENGAGEMENT PROGRAM

CISA is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CISA works to prevent or minimize disruptions to critical information

infrastructure to protect the public, the economy, and government services. CISA leads efforts to protect the Federal ".gov" domain of civilian government networks and to collaborate with the private sector—the ".com" domain—to increase the security of critical networks.

The DHS SLTT Cybersecurity Engagement Program within CISA was established to help non-federal public stakeholders and associations manage cyber risk. The program provides appointed and elected SLTT government officials with cybersecurity risk briefings, information on available resources, and partnership opportunities to help protect their citizens online. Through these and related activities, the program coordinates DHS's cybersecurity efforts with its SLTT partners to enhance and protect their cyber interests. More information on all CISA resources available to support SLTT governments is available at the Resources & Tools page on CISA.gov.

8.13.8. CYBERSECURITY FRAMEWORK

When requesting funds for cybersecurity, applicants are encouraged to propose projects that would aid in implementation of all or part of the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). The CSF 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization, regardless of its size, sector, or maturity, to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes.

Please visit CISA.gov for additional resources that can help public and private sector organizations achieve the outcomes described in the CSF.

8.13.9. LAW ENFORCEMENT SUPPORT OFFICE, OR 1033 PROGRAM

LESO facilitates a law enforcement support program, which originated from the National Defense Authorization Act of Fiscal Year 1997. This law allows the transfer of excess Department of Defense property that might otherwise be destroyed to law enforcement agencies across the United States and its territories.

No equipment is purchased for distribution. All items were excess that had been turned in by military units or had been held as part of reserve stocks until no longer needed. Requisitions cover the array of items used by America's military — clothing, office supplies, tools and rescue equipment, vehicles, small arms, and more. There is no fee for the equipment itself; however, the law enforcement agencies are responsible for the shipping costs.

For additional information on the LESO, see the LESO page on DLA.mil.

9. Nonprofit Security Grant Program

9.1. Program Funding Guidelines and Priorities

NSGP grant recipients (e.g., SAAs) and subrecipients (e.g., nonprofit organizations) may only use NSGP grant funds for the purpose set forth in the grant award and must use funding in a way that is consistent with the statutory authority for the award. See the annual NSGP NOFO for program priorities.

9.1.1. NATIONAL INCIDENT MANAGEMENT SYSTEM IMPLEMENTATION

Recipients receiving NSGP funding must implement NIMS. Recipients must manage resources purchased or supported with FEMA grant funding according to NIMS resource management guidance.

9.2. Nonprofit Security Grant Program Investment Modifications – Changes in Scope or Objective

Changes in scope or objective of the award—whether as a result of intended actions by the recipient or subrecipients—require FEMA's prior written approval, in accordance with 2 C.F.R. § 200.308(c)(1), § 200.407. NSGP is competitive with applications recommended for funding based on threat, vulnerability, consequence, and their mitigation to a specific facility/location. However, consistent with 2 C.F.R § 200.308(c)(1), Change in Scope Notification, FEMA requires prior written approval of any change in scope/objective of the grant-funded activity after the award is issued. *See* 2 C.F.R. § 200.308(b), (c). Scope/objective changes will be considered on a case-by-case basis, provided the change does not negatively impact the competitive process used to recommend NSGP awards. Requests to change the scope or objective of the grant-funded activity after the award is made must be submitted by the SAA via FEMA GO as a Scope Change Amendment. The amendment request must include the following:

- A written request from the NSGP subrecipient on its letterhead, outlining the scope or objective change including the approved projects from the subrecipient's IJ, the funds and relative scope or objective significance allocated to those projects, the proposed changes, and any resulting reallocations as a result of the change of scope or objective;
- An explanation why the change of scope or objective is necessary;
- Validation from the SAA that any deviations from the approved IJ are addressed in the vulnerability assessment submitted by the subrecipient at the time of application; and
- The subrecipient request must also address whether the proposed changes will impact its ability to complete the project within the award's POP.

FEMA will generally not approve NSGP change-of-scope requests resulting from the following situations:

- Subrecipients that relocate their facilities after submitting their application who are requesting a change of scope to allow them to use NSGP funds toward projects at the new facility; or

- Subrecipients that renovate their facilities after submitting their application in cases where the subsequent renovations would affect the vulnerability/risk assessment upon which the IJ is based.

NSGP project funding is based on the ability of the proposed project to mitigate the risk factors identified in the IJ. For this reason, FEMA may reject requests to significantly change the physical security enhancements that are purchased with NSGP funding where FEMA believes approval of the request would change or exceed the scope of the originally approved project. FEMA will consider all requests to deviate from the security project as originally proposed on a case-by-case basis, *consistent with* 2 C.F.R. § 200.308(c)(1).

Subrecipients may not proceed with implementing any scope/objective changes until the SAA receives written approval from FEMA through FEMA GO and until the SAA has made any required subaward modifications.

If a subrecipient is simply making changes to its own budget without impacting the scope or objective of the subaward, and where the budget changes do not involve other prior approval requirements listed in 2 C.F.R. § 200.407, then the subrecipient does not need the prior approval of the SAA or FEMA. *See* 2 C.F.R. § 200.308. Instead, the subrecipient is only required to report to the SAA the budget changes. Similarly, the SAA should report those budget changes to FEMA.

9.3. Pass-Through Requirements

Pass-through funding is required under this program. Awards made to the SAA for the NSGP carry additional pass-through requirements. Pass-through is defined as an obligation on the part of the state to make subawards to selected nonprofit organizations. The SAA must provide funds awarded under NSGP to subrecipients within 45 days of receipt of the funds. A letter of intent (or equivalent) to distribute funds is not sufficient. Award subrecipients that are selected for funding under this program must be provided with funding within 45 days from the date the funds are first made available to the recipient so that they can initiate implementation of approved investments.

For the SAA to successfully meet the pass-through requirement and provide funding to the subrecipients, the SAA must meet the following four requirements:

- There must be some action by the SAA to establish a firm commitment to award the funds to the selected nonprofit organization;
- The action must be unconditional on the part of the SAA (i.e., no contingencies for availability of SAA funds);
- There must be documentary evidence of the commitment of the award of funding to the selected nonprofit organization; and
- The SAA must communicate the terms of the subaward to the selected nonprofit organization.

If a nonprofit organization is selected for an NSGP award and elects to decline the award, the SAA must notify their FEMA Preparedness Officer. The SAA may not re-obligate to another subrecipient without prior approval. “Receipt of the funds” occurs either when the SAA accepts the award or 15 calendar days after the SAA receives notice of the award, whichever is earlier. SAAs are sent notification of NSGP awards via the FEMA GO system. If an SAA accepts its award within 15 calendar days of receiving notice of the award in the FEMA GO system, the 45-calendar day pass-through period will start on the date the SAA accepted the award. Should an SAA not accept the NSGP award

within 15 calendar days of receiving notice of the award in the FEMA GO system, the 45-calendar days pass-through period will begin 15 calendar days after the award notification is sent to the SAA via the FEMA GO system.

It is important to note that the POP start date does not directly affect the start of the 45-calendar day pass-through period. For example, an SAA may receive notice of the NSGP award on Aug. 20, 2023, while the POP dates for that award are Sept. 1, 2023, through Aug. 31, 2026. In this example, the 45-day pass-through period will begin on the date the SAA accepts the NSGP award or Sept. 4, 2023 (15 calendar days after the SAA was notified of the award), whichever date occurs first. The POP start date of Sept. 1, 2023, would not affect the timing of meeting the 45-calendar day pass-through requirement.

10. Surface Transportation Security Grant Programs (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program)

10.1. Program Funding Guidelines and Priorities (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program)

Costs charged to a TSGP, IPR Program, or IBSGP award must be consistent with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, located at 2 C.F.R. Part 200.

- NOTE: Costs charged to an **IPR Program award** must also be consistent with the cost principles in the Federal Acquisition Regulation (FAR) Part 31.2 in lieu of 2 C.F.R. Part 200, Subpart E. Any conflicts between FAR 31.2 and 2 C.F.R. Part 200, Subpart E shall be resolved in favor of the applicable provision in FAR 31.2.

See annual program NOFO for information on program-specific priorities.

10.2. Changes in Scope or Objectives (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program)

All three Surface Transportation Security Grant Programs generally do not allow for scope or objective changes unless there are extenuating circumstances (e.g., the COVID-19 or a similar pandemic preventing activities). FEMA will consider scope/objective changes on a case-by-case basis if extenuating circumstances are present. Please contact your assigned Preparedness Officer for any questions regarding scope changes.

10.3. Security Plan Requirements (Transit Security Grant Program, Intercity Passenger Rail Program, Intercity Bus Security Grant Program)

10.3.1. TRANSIT SECURITY GRANT PROGRAM AND INTERCITY PASSENGER RAIL PROGRAM

The following information regarding security plan requirements is provided in 6 U.S.C. § 1134(c)(2):

Security plans should include the following, as appropriate:

- A prioritized list of all items included in the public transportation agency's[1] security assessment that have not yet been addressed;

[1] For the purposes of this section, the phrase "public transportation agency" includes Amtrak.

- A detailed list of any additional capital and operational improvements identified by DHS or the public transportation agency and a certification of the public transportation agency's technical capacity for operating and maintaining any security equipment that may be identified in such list;

- Specific procedures to be implemented or used by the public transportation agency in response to a terrorist attack including evacuation and passenger communication plans along with appropriate evacuation and communication measures for the elderly and individuals with disabilities;

- A coordinated response plan that establishes procedures for appropriate interaction with state and local law enforcement agencies, emergency responders, and federal officials to coordinate security measures and plans for response in the event of a terrorist attack or other major incident;

- A strategy and timeline for conducting training under 49 C.F.R. § 1570.109(b) and 49 C.F.R. Part 1582;

- Plans for providing redundant and other appropriate backup systems necessary to ensure the continued operation of critical elements of the public transportation agency in the event of a terrorist attack or other major incident;

- Plans for providing service capabilities throughout the agency in the event of a terrorist attack or other major incident in the city or region which the public transportation agency serves;

- Methods to mitigate damage within a public transportation agency in case of an attack on the system, including a plan for communication and coordination with emergency responders; and

- Other actions or procedures as the Secretary of Homeland Security determines are appropriate to address the security of the public transportation agency.

Entities providing transit security (e.g., city/county police department or a transportation agency's own police department) must approve the security plan. The signature of a responsible official from the agency's security provider serves as this approval. Associated documentation of this approval must be provided to DHS/FEMA upon request. In addition, the agency's security provider is encouraged to review the IJs before submission.

An application submitted by an otherwise eligible non-federal entity (i.e., the applicant) may be deemed ineligible when the person that submitted the application is not: 1) a current employee, personnel, official, staff or leadership of the non-federal entity; and 2) duly authorized to apply for an award on behalf of the non-federal entity at the time of application.

Further, the AOR and SA must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and provide an email address unique to the recipient at the time of application and upon any change in assignment during the POP. Consultants or contractors of the recipient are not permitted to be the AOR or the SA of the recipient. It is the sole responsibility of the recipient to keep their points of contact for the organization up-to-date and accurate in all federal systems.

The AOR is responsible for submitting programmatic and financial performance reports, accepting award packages, signing assurances and certifications, and submitting award amendments.

10.3.2. ADDITIONAL AMTRAK REQUIREMENTS

Sections 1512 and 1513 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. §§ 1162 and 1163) require a recipient to complete a vulnerability assessment and develop a security plan. To be eligible for the IPR Program, Amtrak must have developed, or updated, its security plan. The security plan must be based on a security assessment, such as the Baseline Assessment for Security Enhancement (BASE), which is performed by TSA's Surface Transportation Security Inspectors (TSI). This security assessment must have been conducted within the last three years prior to receiving the respective FY's IPR Program award. A copy of the security plan and security assessment must be provided to DHS/FEMA upon request.

10.3.3. INTERCITY BUS SECURITY GRANT PROGRAM REQUIREMENTS

To be eligible for the IBSGP, operators must have developed or updated their organization's Vulnerability Assessment and Security Plan (VASP) that must be based on a security assessment, such as the BASE performed by TSA Surface TSIs. Private operators providing transportation with an over-the-road bus system must have completed or updated their VASP within the past three years before the opening of the respective fiscal year's IBSGP application period. Additionally, a copy of the VASP certification must be submitted along with the application to be considered eligible. Failure to include this certification will result in the application being deemed ineligible. All operators must have completed or updated a VASP as required by Section 1531 of the 9/11 Act (6 U.S.C. § 1181) as follows:

Assessments and security plans should include, as appropriate:

- Identification and evaluation of critical assets and infrastructure, including buses, platforms, stations, terminals, and information systems;
- Identification of vulnerabilities to those assets and infrastructure; and
- Identification of gaps in physical security; passenger and cargo security; the security of programmable electronic devices, computers, or other automated systems that are used in providing over-the-road bus transportation; alarms, cameras and other communications systems and utilities needed for over-the-road bus security purposes, including dispatching systems; emergency response planning; and employee training.

Security plans should also include, as appropriate:

- The identification of a security coordinator having authority to implement security actions, coordinate security improvements, and receive communications from appropriate federal officials regarding over-the-road bus security;
- A list of needed capital and operational improvements;
- Procedures to be implemented or used by the operator in response to a terrorist attack, including evacuation and passenger communication plans that include individuals with access and functional needs;
- The identification of steps taken with state and local law enforcement agencies, emergency responders, and federal officials to coordinate security measures and plans for response to a terrorist attack;

- A strategy and timeline for conducting training to prepare frontline employees for potential security threats and conditions;
- Enhanced security measures to be taken by the operator when the Secretary of Homeland Security declares a period of heightened security risk; and
- Plans for providing redundant and backup systems required to ensure the continued operation of critical elements of the operator's system in the event of a terrorist attack.

For additional information, see the current fiscal year IBSGP NOFO.

10.4. Allowable Cost Guidance

10.4.1. SPECIFIC GUIDANCE ON EXPLOSIVES DETECTION CANINE TEAMS (TRANSIT SECURITY GRANT PROGRAM, INTERCITY PASSENGER RAIL PROGRAM)

Explosives Detection Canine Team Certification

Each Explosives Detection Canine Team (EDCT), composed of one dog and one handler, must be certified by an appropriate, qualified organization. TSA-certified EDCTs will meet or exceed certification standards set by the TSA National Explosives Detection Canine Team Program (NEDCTP). Recipient EDCTs that do not participate in the NEDCTP will be required to certify annually under their respective agency, local, and state regulations. The recipient will maintain certification, utilization, and training data to show compliance in meeting or exceeding those guidelines set forth by the Scientific Working Group on Dog and Orthogonal Detection Guidelines (SWGDOG), as of Sept. 14, 2007, in addition to the requirements set forth in the NOFO.

Explosives Detection Canine Team Submission Requirements

1. The recipient will ensure that a written security procedure plan exists for the safekeeping of all explosive training aids, including safe transportation. The recipient will document the removal, use, and return of explosive training aids used during training exercises or for any other reason. The plan and all documentation must be made available to FEMA upon request;
2. The recipient will comply with requirements for the proper storage, handling, and transportation of all explosive training aids in accordance with the Bureau of Alcohol, Tobacco, Firearms and Explosives' Publication 5400.7 (ATF P 5400.7) (09/00), Federal Explosive Law and Regulation;
3. The recipient will ensure that certified EDCTs are available to respond to situations 24 hours a day, 7 days per week on an on-duty or off-duty on-call basis. If TSGP- or IPR Program-funded EDCTs are not available, other non-TSGP or non-IPR Program funded EDCTs may be utilized for this response. The intent is to provide maximum coverage during peak operating hours and to maintain the ability to promptly respond to threats that affect public safety or mass transit operations;
4. EDCTs under this grant are single purpose and will be trained to detect "live" explosives only, not "simulated" explosives. EDCTs must not have received previous training to detect any other substances;

5. The recipient will ensure that each EDCT receives on-site proficiency training at a minimum of four hours per week per duty cycle. This training shall include, but not be limited to, mass transit passenger cars, terminals/platforms, luggage, freight/warehouses, and vehicles. Complete, detailed, and accurate training records must be maintained for all proficiency training conducted by each EDCT. These records must be made available to FEMA upon request;

6. The recipient will conduct appropriate training or other canine activities, within view of the public, to increase public awareness of EDCTs and provide a noticeable deterrent to acts which affect public safety or mass transit operations. The recipient will also ensure that such activities include, over a period, a presence in operational areas of the mass transit system during peak and off-peak hours. The recipient agrees that EDCTs will be utilized in the field at least 80% of their duty time, annually;

7. The recipient will provide safe and sanitary kennel facilities for program canines, and these costs may be allowable with prior approval by FEMA. This applies to kenneling canines at a mass transit system, handlers' residences, or commercial boarding facilities. Canines must not be left in makeshift accommodations or without proper supervision, protection, and care. The recipient will ensure that canines are transported on-duty and off-duty in vehicles configured with adequate temperature control, padding, and screening to ensure proper health, safety, and security; and

8. The recipient will ensure that adequate routine and emergency veterinary care are provided for all canines.

Note: FEMA reserves the right to conduct an on-site operational and record review upon 48-hour notice to ensure compliance with applicable federal regulations.

10.4.2. CAPITAL (CONSTRUCTION) PROJECTS GUIDANCE (TRANSIT SECURITY GRANT PROGRAM, INTERCITY PASSENGER RAIL PROGRAM, INTERCITY BUS SECURITY GRANT PROGRAM)

Applicants must obtain written approval from FEMA before using any program funds for construction or renovation projects. When applying for construction funds, including communications towers, the recipient must submit evidence of approved zoning ordinances, architectural plans, and any other locally required planning permits. Additionally, the recipient is required to submit a SF-424C Form and budget detail citing the project costs and a SF-424D Form for standard assurances for the construction project.

Additional guidance for Transit Security Grant Program Capital (Construction) Projects:

Capital expenditures are defined in 2 C.F.R. § 200.1 as expenditures to acquire capital assets or expenditures to make additions, improvements, modifications, replacements, rearrangements, reinstallations, renovations, or alterations to capital assets that materially increase their value or useful life. Use of capital expenditures must comply with 2 C.F.R. § 200.439. See Section 4.5.1 "Construction and Renovation" for more information.

11. Port Security Grant Program

11.1. Program Funding Guidelines and Priorities

PSGP grant recipients may only use PSGP grant funds for the purpose set forth in the grant award and must use funding in a way that is consistent with the statutory authority for the award. See the annual PSGP NOFO for program Priorities.

11.2. Allowable Cost Guidance

11.2.1. SPECIFIC GUIDANCE ON EXPLOSIVES DETECTION CANINE TEAMS

Explosives Detection Canine Team Certification

Each EDCT, composed of one dog and one handler, must be certified by an appropriate, qualified organization. Canine (K-9) and handler should receive an initial basic training course and weekly maintenance training sessions thereafter to maintain the certification. The basic training averages ten weeks for the canine team (K-9 and handler together) with weekly training and daily exercising. Comparable training and certification standards, such as those promulgated by the TSA Explosive Detection Canine Program, the National Police Canine Association (NPCA), the U.S. Police Canine Association (USPCA), or the International Explosive Detection Dog Association (IEDDA), may be used to meet this requirement. Certifications and training records will be kept on file with the recipient and made available to FEMA upon request.

Explosives Detection Canine Team Submission Requirements

PSGP recipients are required to submit a written plan or standard operating procedure (SOP) that describes EDCT deployment policy including visible and unpredictable deterrent efforts and on-call EDCTs rapid response times. Recipients who are subject to the maritime security regulations contained in 33 C.F.R. Parts 104 (vessel security) or 105 (facility security), shall submit a Vessel Security Plan (VSP) or Facility Security Plan (FSP) amendment detailing the inclusion of a (K-9) explosive detection program into their security measures to the USCG for review and approval. The relevant portion of any USCG-approved VSP or FSP, or any agency specific security plan or SOP must be made available to FEMA and USCG upon request. The recipient will comply with requirements for the proper storage, handling, and transportation of all explosive training aids in accordance with the Bureau of Alcohol, Tobacco, Firearms and Explosives' Publication 5400.7 (ATF P 5400.7) (09/00), *Federal Explosive Law and Regulations*.

Additional Explosives Detection Canine Team Resources Available for Canine Costs

The PSGP, while providing the ability to defray some start-up costs, does not cover any recurring costs associated with EDCT programs. FEMA strongly encourages applicants to investigate their eligibility under other programs, and potential exclusions, when developing their K-9 programs.

11.2.2. MARITIME DOMAIN AWARENESS

The maritime domain is defined as "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances." PSGP recipients are encouraged

to familiarize themselves with this National Strategy. Homeland Security Presidential Directive-13 (NSPD-41/HSPD-13) (Maritime Security Policy, Dec. 21, 2004). According to the National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security (Oct. 2005), "Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States. MDA is a key component of an active, layered maritime defense in depth. It will be achieved by improving our ability to collect, fuse, analyze, display, and disseminate actionable information and intelligence to operational commanders." *Id.* at ii.

11.2.3. CAPITAL (CONSTRUCTION) PROJECTS GUIDANCE

Recipients must obtain written approval from FEMA before using any PSGP funds for construction or renovation projects.

Additionally, PSGP funding may not be used to construct buildings or other physical facilities that are not constructed under terms and conditions consistent with the requirements of section 611(j)(9) of the Stafford Act (42 U.S.C. § 5196(j)(9))[2] which requires compliance with the Davis-Bacon Act (codified as amended at 40 U.S.C. §§ 3141 *et seq*.) for PSGP funded projects. Grant recipients must ensure that their contractors or subcontractors for construction projects pay workers no less than the prevailing wages for laborers and mechanics employed on projects of a character similar to the contract work in the civil subdivision of the state in which the work is to be performed. See Section 4.6 "Davis-Bacon Act Compliance" for more information.

Recipients must also comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA). None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States. Please see Section 6.7 "Financial Assistance Programs for Infrastructure" and the PSGP NOFO for more information.

The following types of construction and renovation projects are allowable under PSGP, provided they address a specific vulnerability or need identified in an AMSP or otherwise support the maintenance/sustainment of capabilities and equipment acquired through PSGP funding:

- Maritime Command and Control Centers;
- Interagency Operations Centers (IOCs) for maritime security;
- Port Security Emergency Communications Centers;
- Buildings to house generators that support maritime security risk mitigation;
- Maritime security risk mitigation facilities (e.g., dock house, ramps, and docks for existing port security assets);

[2] While the Maritime Transportation Security Act of 2002, as amended at 46 U.S.C. § 70107(b)(2), requires that such activities are carried out consistent with Section 611(j)(8) of the Stafford Act, a subsequent amendment to the Stafford Act by section 3 of Pub. L. No. 109-308 in 2006 redesignated the text of Section 611(j)(8) to 611(j)(9). The cross reference in the Maritime Transportation Security Act of 2002 has not been updated.

- Hardened security fences/barriers at access points;
- Any other building or physical facility that enhances access control to the port/Maritime Transportation Security Act (MTSA) facility area; and
- PSGP funding may be used to purchase and/or upgrade a barge to support a staging area for maritime/port security patrols or maritime security risk mitigation responses. (Certain areas throughout the Nation may require a barge that can be permanently anchored or moored in certain areas to support maritime security risk mitigation activities.)

To be considered eligible for funding, the construction of fusion centers, operations centers, or communications centers must offer a port wide benefit and support information sharing and operational coordination among regional interagency and other port security partners. Applicants are reminded that the POP is 36 months. Eligible costs for construction or renovation projects may not exceed $1 million (federal share) per project, which may not exceed 10% of the total amount of the award, as stated in 46 U.S.C. § 70107(b)(2)(A) and (B) (Section 102 of the Maritime Transportation Security Act of 2002, Pub. L. 107-295, as amended). Grant recipients are not permitted to use PSGP funds for construction projects that are eligible for funding under other federal grant programs. PSGP funds may only be used for construction activities directly related to maritime security risk mitigation enhancements.

All construction or renovation projects require EHP review. See Section 4.5 "Environmental Planning and Historic Preservation Compliance" for more information.

11.3. Port-Wide Risk Management Plans

Port areas with existing Port Wide Risk Mitigation Plans (PRMPs) are encouraged to maintain their PRMPs and use them to identify projects that will serve to address remaining maritime security vulnerabilities. These ports are also encouraged to develop or maintain a Business Continuity and Resumption of Trade Plans (BCRTP). For purposes of regional strategic and tactical planning, these plans must take into consideration all port areas covered by their AMSP, align with the port area's AMSP, consider the entire port system strategically as a whole, and identify actions designed to effectively mitigate security risks associated with the system's maritime critical infrastructure and key resources.

11.4. Port Security Grant Program Investment Modifications

The purpose of the grant award is to implement projects pursuant to the authorities at 46 U.S.C. § 70107. Under extreme circumstances, a recipient may reallocate award funds from one project to another with prior written approval from FEMA and in a manner consistent with 2 C.F.R. § 200.308 if it does not change the overall scope or objective of the award. Circumstances include, but are not limited to, an inability to complete the original project, disaster events perpetuating an immediate need to reprioritize funds, and changes in regulatory requirements. A recipient must explain the deviation from the original project- including why it is deviating from or scaling down the original project and what specific circumstances that occurred after the time of its award that necessitate the reallocation request- in its reallocation request. The recipient must also identify how the reallocation request aligns with PSGP priorities and the recipient's original application and the award's scope of work. Due to legal limitations, reallocation requests that would change the scope of the overall project(s) are not permitted. FEMA will also coordinate such reallocation requests with the USCG Captain of the Port (COTP), and these requests must be verified and supported by the COTP as

essential in addressing Port Area priorities. Please also see the relevant PSGP NOFO regarding cost share requirements including the implications if the project costs are less than what was applied for.

12. Emergency Management Performance Grant Program

12.1. Alignment of the Emergency Management Performance Grant Program to the National Preparedness System

The EMPG Program contributes to the implementation of the National Preparedness System by supporting the building, sustainment, delivery, and maintenance of core capabilities. Core capabilities are essential for the execution of critical tasks for each of the five mission areas outlined in the Goal. The EMPG Program's allowable costs support efforts to build and sustain core capabilities across the Prevention, Protection, Mitigation, Response, and Recovery mission areas described in the Goal.

FEMA requires recipients to prioritize grant funding to demonstrate how EMPG Program-funded investments support the following:

- Building or sustaining those capabilities that are identified as high priority through the THIRA/SPR process and other relevant information sources, such as:
  - AARs following exercises or real-world events;
  - Audit and monitoring findings;
  - Hazard Mitigation Plans; and
  - Other deliberate planning products.
- Closing capability gaps that are identified in the state or territory's most recent SPR.

To better understand the relationship between building capabilities and closing capability gaps, refer to CPG 201, Third Edition. In advance of issuing the EMPG Program awards, FEMA Regional Administrators will identify individual regional priorities based on their unique knowledge of each region's preparedness and emergency management needs and will share those priorities with the states and territories within their region. The final priorities will be identified and mutually agreed to by the state/territory and Regional Administrator through a collaborative negotiation process. Ideally, all EMPG Program-funded projects, as outlined in the approved EMPG Program Work Plan, will support the priorities identified through this collaborative approach. See the EMPG Program Work Plan template in the EMPG Program NOFO for additional guidance.

FEMA continues to place emphasis on capabilities that address the greatest risks to the security and resilience of the United States. When applicable, funding should support deployable assets that can be used anywhere in the Nation through automatic assistance and mutual aid agreements, including, but not limited to, the EMAC. The EMPG Program supports investments that improve the ability of jurisdictions nationwide to:

- Prevent a threatened or an actual act of terrorism;
- Protect our citizens, residents, visitors, and assets against the greatest threats and hazards;
- Mitigate the loss of life and property by lessening the impact of future disasters;

- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident; or
- Recover through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident.

The core capabilities contained in the Goal are highly interdependent and require the use of existing preparedness networks and activities to improve training and exercise programs, innovation, and appropriate administrative, finance, and logistics systems.

12.2. Implementation of the National Preparedness System

12.2.1. IDENTIFYING AND ASSESSING RISK AND ESTIMATING CAPABILITY REQUIREMENTS

By Dec. 31, 2022, recipients were required to complete a THIRA/SPR that addresses all 32 core capabilities and is compliant with CPG 201, Third Edition. Recipients are required to submit a THIRA every three years to establish a consistent baseline for assessment. 2022 was the start of the new three-year THIRA/SPR cycle and baseline assessment year for existing recipients. Any new grant recipients during future CYs, for which the THIRA/SPR requirement applies, will start their new three-year THIRA/SPR cycle and baseline assessment year in that year. Specific guidance on the requirements for each core capability is provided through program implementation support and supplemental guidance, as some core capabilities have fewer reporting requirements than others. Recipients must continue to respond to a series of planning-related questions as part of the THIRA/SPR process.

While the THIRA is only required every three years, jurisdictions are required to submit an SPR annually. The submission deadline is Dec. 31 each year (as applicable). For additional guidance on the THIRA/SPR, please refer to CPG 201, Third Edition. Recipients are also encouraged to refer to the Preparedness Toolkit, which is an online portal that provides the whole community with tools to aid in implementing all six areas of the National Preparedness System.

Reporting

In each EMPG Program recipient's BSIR, the recipient must describe how expenditures support building capability, closing capability gaps, or sustaining capabilities identified in the THIRA/SPR process. EMPG Program recipients will, on a project-by-project basis, check one of the following:

- Building a capability with EMPG Program funding; or
- Sustaining a capability with EMPG Program funding.

Building and Sustaining Core Capabilities

Recipients must describe how proposed EMPG Program-funded projects will close capability gaps or sustain capabilities identified through the THIRA/SPR process, particularly SPR Step 2 (see CPG 201, Third Edition), or other relevant information sources that identify capability needs. See the EMPG Program Work Plan template in the EMPG Program NOFO for additional guidance and requirements.

12.2.2. NATIONAL INCIDENT MANAGEMENT SYSTEM IMPLEMENTATION

EMPG Program recipients must use standardized resource management concepts for resource typing, credentialing, and an inventory to facilitate the effective identification, dispatch, deployment, tracking, and recovery of resources. EMPG Program funds may be used for NIMS implementation; specifically, to meet the requirements described in the NIMS Implementation Objectives for Local, State, Tribal, and Territorial Jurisdictions.

Reporting

- Recipients will answer questions in the applicable secondary NIMS assessment portion of the URT as part of a jurisdiction's THIRA/SPR submission. This involves reporting on the status of the qualification system used within the jurisdiction and sub-jurisdictions, as outlined in the EMPG Program NOFO.

- Reporting will also be through a review by the FEMA Regional NIMS Coordinators during annual TA visits with the states, Tribal Nations, and territories within their regions.

12.2.3. NATIONAL QUALIFICATION SYSTEM IMPLEMENTATION

For FY 2023 and going forward, as a post-award requirement, all recipients in the 50 states and District of Columbia must work toward achieving the Phase 1 NQS Implementation Objectives outlined in the table below and must, at a minimum, execute the Implementation Plan they developed in FY 2022 as part of the Phase 0 NQS Implementation Objectives. Jurisdictions that began implementation in FY 2023 shall have designed and adopted organizational qualification system procedures, a certification program and credentialing standards for incident workforce personnel in alignment with the NIMS Guideline for the NQS. All other jurisdictions (including territories and EMPG Program subrecipients) are required to work toward implementation of NQS by developing an Implementation Plan, using the FEMA-provided two-page template referenced in the table below.

For all states and territories, the following requirements shall apply:

- At a minimum, only **EMPG Program-funded deployable personnel, as determined by each recipient organization,** will be required to meet NQS certification requirements.

- Recipients and subrecipients will be considered in compliance with the NQS requirements as long they are **working toward implementing** the NQS Implementation Objectives as outlined in the table below.

- The expected completion date for each phase of the NQS Implementation Objectives is Dec. 31 of the applicable CY.

Additional NQS Implementation Guidance can be found at the NQS Supplemental Documents page on FEMA.gov.

Table 8: National Qualification System Implementation Phase Objectives

Phase 0: NQS Implementation Objectives for CY 2022	Example Indicators
▪ Only the 50 States, the District of Columbia and Puerto Rico shall work toward implementation of NQS by developing an Implementation Plan using the FEMA-provided two-page template. ▪ The Implementation Plan will identify a jurisdiction's timeline for implementing NQS by CY 2025. ▪ All other jurisdictions are encouraged to begin working toward identifying, at a minimum, frequently deployed positions and implementation but will not be required until CY 2023.	▪ Completion of a jurisdiction implementation plan. ▪ Identification of implementation challenges.
Phase 1: NQS Implementation Objectives for CY 2023	**Example Indicators**
▪ All jurisdictions shall work toward implementation of NQS by developing an Implementation Plan using the FEMA-provided two-page template. ▪ Jurisdictions that began implementation in CY 2022 shall have designed and adopted organizational qualification system procedures, a certification program, and credentialing standards for incident workforce personnel in alignment with the NIMS Guideline for the NQS.	▪ Completion of a jurisdiction implementation plan. ▪ Identification of implementation challenges. ▪ Qualification policies and procedures approved by the jurisdiction. Procedures may include: ○ Establishment of a Qualification Review Board or equivalent review processes for incident workforce personnel qualifications. ○ Individual and team coach and evaluation processes for incident workforce personnel qualifications.

Phase 2: NQS Implementation Objectives for CY 2024	Example Indicators
▪ All jurisdictions shall have designed and approved organizational qualification system procedures, certification program, and credentialing standards for incident workforce personnel in alignment with the NIMS Guideline for the NQS. ▪ Jurisdictions that began implementation in CY 2022 shall have issued position task books (PTBs) to incident workforce personnel, as designated by the jurisdiction, and ensure incident workforce personnel show progress in working toward task endorsements and minimum training requirements. ▪ In CY 2024, all jurisdictions partially satisfy the requirement by ensuring designated incident workforce personnel meet the minimum training requirements from the Job Title/Position Qualification. ▪ Jurisdictions shall use a resource management or qualification tool system to track the qualification, certification, and credentialing of incident workforce personnel.	▪ Qualification policies and procedures approved by the jurisdiction. ▪ Minimum criteria that trainees must meet to be qualified in a specific position is outlined in the NQS Job Title/Position Qualification. ▪ PTB issuance and completion data. ▪ Adoption of a resource management system, such as OneResponder: a web-based application hosted in a cloud environment. It allows Authority Having Jurisdictions (AHJ) to manage qualifications of personnel.
Phase 3: NQS Implementation Objectives for CY 2025	**Example Indicators**
▪ All jurisdictions shall have issued PTBs to designated incident workforce personnel and ensure incident workforce personnel show progress in working toward task endorsements and minimum training requirements.	▪ PTB issuance and completion data.

Reporting

Data collection and reporting on NQS implementation will be addressed via the following:

- NIMS secondary assessment questions on the URT. This involves reporting on the status of the qualification system used within the jurisdiction and sub-jurisdictions.

- Review by the Regional NIMS Coordinators during annual TA visits with the states, Tribal Nations, and territories within their regions.

12.3. Logistics Planning

12.3.1. DISTRIBUTION MANAGEMENT PLANS

EMPG Program recipients are required to develop and maintain a Distribution Management (DM) plan as an annex to their existing EOP. CPG 101 v3.1 provides guidance on the fundamentals of planning and development of EOPs. The Distribution Management Plan Guide 2.0 released in Jan. 2022 provides information on how to develop the DM plan annex, key DM plan components, how to review and update a DM plan, and how FEMA reviews and evaluates the plans.

A state/territory should submit its DM plan as both a Word document and PDF to its FEMA Regional Grants Division. The maturity level of the plan may vary by state/territory, but the recipient is required to submit a DM plan that accurately reflects the state or territory's current capabilities and capacity to distribute resources to survivors after a disaster and addresses the following components: Requirements Defining; Resource Ordering; Distribution Methods; Inventory Management; Transportation; Staging; and Demobilization.

The DM plan must be reviewed by recipients on an annual basis and updated as necessary by Sept. 30 of each CY. In the applicable secondary CPG 101 assessment portion of the online URT, jurisdictions capture whether they have developed and incorporated a DM plan in their EOP.

- The DM plan should focus on the distribution of commodities and supplies such as food, water, generators, and tarps to survivors following a disaster.
- The DM plan should address strategies/plans for:
  - Requirements Defining;
  - Resource Ordering;
  - Distribution Methods;
  - Inventory Management;
  - Staging Areas;
  - Transportation; and
  - Demobilization.

FEMA Regional Logistics Branch staff will work with EMPG Program recipients to provide TA during the development and maintenance of their DM plans and to ensure all recipients have effective DM plans capable of integrating with federal, NGOs, private sector, and SLTT stakeholders during major disasters. Recipients should refer to the Distribution Management Plan Guidance found in the Planning Guides page on FEMA.gov for additional guidance.

12.3.2. ADDITIONAL LOGISTICS PLANNING RESOURCES

FEMA recommends that EMPG Program recipients use the following resources in developing their DM plan. To learn more about these programs and documents, or for any questions, please contact the Logistics Section Chief from your FEMA Region.

- **The Logistics Capability Assessment Tool 2 (LCAT2) Flyer:** The LCAT2 Flyer provides an overview of the LCAT2, how it is beneficial, how the LCAT process works, and how to obtain an LCAT2. For more information on the LCAT2, contact your FEMA Regional Logistics Branch Chief.

- **Points of Distribution (PODs) Training:** FEMA Logistics developed a comprehensive POD training to assist states in developing actionable emergency distribution plans and understanding associated challenges. Additional information, including an explanatory DVD, POD guide, and online exam, are available on EMI's website at the IS-26: Guide to Points of Distribution page.

- **Interagency Logistics (IL) Training:** This basic IL training course (Interagency Logistics Training, E8540) familiarizes participants with the IL concepts of planning and response. The course also provides an overview of IL Partner disaster response organizations, discusses parameters for logistics support coordination, and creates a whole community forum to exchange the best logistics practices. Recipients may find more information on this and other courses by visiting the EMI Courses & Schedules website.

- **Other Logistics Planning Resources:** Recipients will find additional planning guidance at the Planning Guides page on FEMA.gov. Specific to logistics planning, CPG 101 v3.1 provides guidance on how to incorporate logistics into EOPs. Additionally, the Supply Chain Resilience Guide provides emergency managers with recommendations and best practices on how to analyze local supply chains and work with the private sector to enhance supply chain resilience using a five-phased approach.

Reporting

Annual DM plan reviews will be reported in the PPR for the quarter ending Sept. 30 of the most recently awarded EMPG Program. Reviews that result in an update must be submitted to the Regional Grants Division Director or Regional EMPG Program Manager for review by regional logistics staff. The regional logistics staff will review and rate the plans using the latest FEMA Distribution Management Plan Guide 2.0.

12.4. Evacuation Planning

EMPG Program recipients should review and update their EOP in accordance with CPG 101 v3.1. Recipients are strongly encouraged to include an evacuation plan or annex as part of their EOP as well as plans to exercise and validate the evacuation plan and capabilities. At a minimum, recipients should incorporate the National Response Framework's (NRF's) Mass Evacuation Incident Annex's planning considerations, and other FEMA documents related to evacuation planning, when developing their own Evacuation Plan or Annex. See the NRF, Fourth Edition (October 2019) and NRF Mass Evacuation Incident Annex (June 2008). Additional National Preparedness resources are available at National Preparedness and Planning Guides pages on FEMA.gov. Specific to evacuation planning, the Evacuation and Shelter in Place Guidance identifies relevant concepts, considerations, and principles that can inform jurisdictions in planning for evacuation and/or shelter-in-place protective actions.

12.5. Disaster Housing Planning

12.5.1. STATE-LED DISASTER HOUSING TASK FORCE

Based on lessons learned from recent disasters, FEMA strongly encourages EMPG Program recipients to establish a State-Led Disaster Housing Task Force (SLDHTF) plan as part of their EOP or as a standalone document and update their plan at least once every two years.

SLDHTFs lead and coordinate state, local, private sector, and community-based actions to assess housing impacts, identify appropriate post-disaster housing options, and establish processes for expediting post-disaster housing delivery. SLDHTF plans should clearly identify the roles, responsibilities, composition, and mobilization procedures for the SLDHTF, and how the SLDHTF integrates into the incident command structure. To have a successful SLDHTF plan, FEMA encourages recipients to establish a State Disaster Recovery Coordinator (SDRC).

- Complete the State Housing Strategy Template.

12.5.2. DISASTER HOUSING EXERCISES

SLTT governments are encouraged to exercise and validate their long-term sheltering and housing stabilization plans as part of an existing exercise program. This includes:

- Validating the organizational structure of the Housing Task Force and internal readiness capabilities to address post-disaster housing recovery.
- Validating disaster housing communication plans and procedures that coordinate and integrate the activities and information generated by internal/external partners.
- Validating data systems, security, and exchange protocols.
- Validating planned actions and milestones transitioning from emergency sheltering to temporary housing to permanent housing and long-term recovery.

12.5.3. ADDITIONAL DISASTER HOUSING PLANNING RESOURCES

SLTT governments are encouraged to review the planning guidance available at the Planning Guides page on FEMA.gov. The Planning Guides page includes Planning Considerations: Disaster Housing Guidance for State, Local, Tribal and Territorial Partners (April 2025), which supplements CPG 101 v3.1. It provides guidance on national housing priorities, types of housing, key considerations, and housing-specific planning recommendations for SLTT jurisdictions to use, in conjunction with the Six-Step Planning Process described in CPG 101 v3.1, to develop or improve disaster housing plans.

12.6. State Disaster Recovery Coordinator

The Pre-Disaster Recovery Planning Guide helps states prepare for recovery by developing pre-disaster recovery plans that follow a process to engage members of the whole community, develop recovery capabilities, and create an organizational framework for recovery efforts.

FEMA strongly recommends that EMPG Program recipients include pre-disaster recovery planning as part of their State Readiness and Preparedness efforts by establishing an SDRC. An effective pre-disaster recovery plan and process is crucial to help recipients prepare for major disaster incidents

and recover effectively. Recipients are encouraged to use the Pre-Disaster Recovery Planning Guide to help inform their identification and establishment of a SDRC. The SDRC position should be included in the State Administrative Plan with the following responsibilities:

- Development of the pre-disaster recovery plan, including state-level leadership and structure, formation of communication channels, multi-agency coordination, and building whole-community partnerships to support recovery efforts.
- Set the stage for necessary strategic, operational, and tactical post-disaster planning, actions, and processes.
- Maximize impact of federal, private sector, and nongovernmental dollars to enable recovery and resilience.
- Accelerate the delivery of resources, including funding and TA, to disaster-impacted communities.
- Enable state leadership to better organize and identify gaps in the state's recovery capabilities.

12.7. Disaster Financial Management Policies and Procedures

Lessons learned from recent hurricane seasons and wildfires demonstrate the need for impacted jurisdictions to improve their ability to immediately track and account for disaster costs. Disaster financial management includes policies and procedures that work to recover expenses pertaining to damage, emergency protective measures, and debris management during and after a disaster. These policies and procedures include, but are not limited to, those supporting eligible contract costs and force account labor, materials, and equipment.

12.7.1. STATE ADMINISTRATIVE PLAN

FEMA strongly recommends that EMPG Program recipients include disaster financial management planning as part of their State Administrative Plan. An effective disaster financial management plan and process is crucial to help recipients prepare for declarations of emergencies or major disasters and plan for reimbursement. The table below details the processes that should be included in the State Administrative Plan and recommendations on where they should be placed.

Table 9: State Administrative Plan Guidance

State Administrative Plan Section Recommendations	Processes
▪ Section V Part D: Project Funding and Reimbursement ▪ Section V Part G: Records and Reports	▪ A process to ensure subrecipients are tracking and documenting disaster costs necessary for federal reimbursement, such as receipts, invoices, procurement documents, contracts, and insurance coverage/claims

State Administrative Plan Section Recommendations	Processes
▪ Section V Part D: Project Funding and Reimbursement ▪ Section V Part G: Records and Reports	▪ A process to document disaster cost operations such as labor, equipment, and materials that are allowable under federal requirements
▪ Section V Part D: Project Funding and Reimbursement	▪ A process to ensure that subrecipients are not receiving a duplication in benefits
▪ Section IV Part B: Organization and Staffing	▪ A process to ensure pre-disaster contracts and procurement strategies are in place, if necessary

Additionally, recipients are encouraged to use EMPG Program funds for training that develops, delivers, and exercises disaster financial management procedures.

12.7.2. DISASTER FINANCIAL MANAGEMENT RESOURCES

Recipients are encouraged to use the following resources to inform their disaster financial management planning efforts:

- **State Administrative Plan Template:** Recipients are recommended to use the State Administrative Plan template found on FEMA's Public Assistance webpage to inform their planning efforts. The template includes example structure and content as a model for states to create their own Administrative Plan.

- **Public Assistance Program and Policy Guide:** The Public Assistance Program and Policy Guide (PAPPG) combines all Public Assistance policy into a single volume and provides an overview of the Public Assistance program implementation process.

- **Public Assistance Frequently Asked Questions and Guidance:** Recipients are encouraged to view the Public Assistance Frequently Asked Questions and guidance found on the Public Assistance webpage to assist with disaster financial management planning efforts. The webpage provides information pertaining to documentation, Public Assistance grant funding eligibility, and hazard mitigation and can be found at the Public Assistance Fact Sheets, Job Aids, and FAQs page on FEMA.gov.

- **DHS OIG Audit Tips:** Recipients are recommended to consult the DHS OIG report, *Audit Tips for Managing Disaster-Related Project Costs* (OIG-17-120-D) for further assistance in documenting and accounting for disaster-related costs. This report is informed by OIG audit findings and can assist recipients in addressing issues that are frequent findings in disaster-related audits.

- **Disaster Financial Management Guide:** The Disaster Financial Management Guide provides guidance for SLTT partners on establishing and implementing sound disaster financial management practices.

- PDAT Training and Resources: The PDAT provides training and other resources to assist grant recipients in their efforts to comply with federal procurement standards.

12.8. Training and Exercises

12.8.1. INTEGRATED PREPAREDNESS PLAN

Recipients are expected to engage senior leaders and other whole community stakeholders to identify preparedness priorities specific to training and exercise needs, which will guide development of a state/territory multi-year IPP. Like the EMPG Program Work Plan development process, these priorities should be informed by various factors, including jurisdiction-specific threats and hazards (i.e., the THIRA); areas for improvement identified by real-world events and exercises (i.e., AAR); external requirements such as stakeholder preparedness reviews (i.e., SPR), homeland security policy, and industry reports; and accreditation standards, regulations, or legislative requirements. Recipients must document these priorities, in conjunction with the Work Plan development process, and use them to deploy a schedule of preparedness events and activities in the IPP. Information related to IPPs and IPPWs can be found on the HSEEP page on FEMA.gov and FEMA's Preparedness Toolkit. FEMA Regional staff can provide TA for IPP and IPPW development.

Recipients should ensure that their EMPG Program Work Plans and IPPs align with and are complementary to one another and are used in tandem to support shared priorities for building and sustaining the state/territory's preparedness capabilities. Recipients should include planning, training, and exercise projects in their EMPG Program Work Plan that support priorities included in their IPP. The current multi-year IPP must be submitted to the Regional EMPG Program Manager before Jan. 31 of each year. Regional Program Mangers will ensure a copy of the IPP is sent to hseep@fema.dhs.gov.

This will help ensure that priorities for both the IPP and EMPG Program Work Plan are based on building capability and/or closing capability gaps documented in their THIRA/SPR and other relevant sources of information. For example, if a recipient included Logistics and Distribution Management, Resilient Communications, and Housing as priorities for its IPP, those should also be priorities in its EMPG Program Work Plan. Additionally, IPPs should include all planning, training, and exercise activities funded by the EMPG Program as well as activities funded by other sources. This inclusion will ensure that recipients' preparedness projects, investments, and activities are concentrated, focused, and oriented toward closing gaps related to their top priorities, regardless of funding source.

12.8.2. VALIDATING CAPABILITIES THROUGH EXERCISES

All recipients are required to develop and maintain a progressive exercise program consistent with HSEEP guidance in support of the NEP. The NEP serves as the principal exercise mechanism for examining national preparedness and measuring readiness. The NEP is a two-year cycle of exercises across the nation that validates capabilities in all preparedness mission areas. The two-year NEP cycle is guided by Principals' Strategic Priorities, established by the National Security Council, and informed by preparedness data from jurisdictions across the Nation.

The NEP provides exercise sponsors the opportunity to receive exercise design and delivery assistance, tools and resources, enhanced coordination, and the ability to directly influence and inform policy and preparedness programs. If you have any questions or would like to request assistance through the NEP, please visit the NEP website or reach out to the NEP directly at NEP@fema.dhs.gov.

The exercises and priorities outlined in the IPP and all EMPG Program-funded exercises must be included in the current fiscal year EMPG Program Work Plan. To avoid duplicate reporting,

applicants/recipients are not required to report EMPG Program-funded personnel costs associated with exercises in the EMPG Program Work Plan. See the EMPG Program Work Plan template in the EMPG Program NOFO for additional guidance.

12.8.3. TRAINING

Like the exercise guidance above, training activities should align to a current, multi-year IPP developed through an annual IPPW and build from training gaps identified in the THIRA/SPR and work plan development process. Further guidance concerning the IPP and the IPPW can be found at the HSEEP Resources page on Preparedness Toolkit.

Through the NPD's training and education enterprise, consisting of CDP, EMI, and NTED's partnerships with the NDPC, RDPC, NCPC, CTG partners, and the Center for Homeland Defense and Security, FEMA develops and delivers training and education programs to increase capabilities, reduce risk, and build resilient communities. More than 680 tuition-free courses are offered to members of SLTT communities. By accessing the National Preparedness Course Catalog, users will find all courses to include EMI training and includes links to the basic, advanced, and executive emergency management academies.

12.8.4. FEMA'S NATIONAL PREPAREDNESS COURSE CATALOG

Training should foster the development of a community-oriented approach to emergency management that emphasizes engagement at the community level, strengthens best practices, and provides a path toward building sustainable resilience, all of which is included in the curriculum of the EMI Basic Academy. The EMI Basic Academy provides a foundational education in emergency management as a way for emergency managers to begin or advance their career. The goal of the Basic Academy is to support the early careers of emergency managers through a training experience combining knowledge of all fundamental systems, concepts, and practices of cutting-edge emergency management.

EMPG Program funds used for training should support the nationwide implementation of NIMS. The NIMS Training Program establishes a national curriculum for NIMS and provides information on NIMS courses. Recipients are encouraged to place emphasis on the core competencies as defined in the NIMS Training Program. NIMS is also included in the curriculum of the EMI Basic Academy. The NIMS Training Program can be found at NIMS Implementation and Training.

All EMPG Program-funded personnel are expected to be trained emergency managers (see Section 12.2.3 "National Qualification System Implementation"). All EMPG Program-funded personnel must complete *either* the Independent Study courses identified in the Professional Development Series, *or* the National Emergency Management Basic Academy delivered either by EMI or at a sponsored SLTT, regional, or other designated location. Further information on the National Emergency Management Basic Academy and the Emergency Management Professional Program (EMPP) can be found at the EMPP page on EMI's website. A complete list of Independent Study Program Courses may be found at the Independent Study page on EMI's website.

In addition to training activities aligned to and addressed in the IPP, all EMPG Program-funded personnel (including full- and part-time SLTT recipients and subrecipients) must complete the following training requirements and record proof of completion:

1. NIMS Training, Independent Study (IS)-100 (any version), IS-200 (any version), IS-700 (any version), and IS-800 (any version)[3]; **and**

2. Professional Development Series (PDS) **or** the EMPP Basic Academy courses listed in the table below.

Table 10: PDS or EMPP Basic Academy Courses[4]

PDS **Professional Development Series**	**Basic Academy** **Basic Academy Pre-requisites and Courses**
IS-120: An Introduction to Exercises	IS-100: Introduction to the Incident Command System
IS-230: Fundamentals of Emergency Management	IS-700: National Incident Management System (NIMS)-An Introduction
IS-235: Emergency Planning	IS-800: National Response Framework, An Introduction
IS-240: Leadership and Influence	IS-230: Fundamentals of Emergency Management
IS-241: Decision Making and Problem Solving	E/L101: Foundations of Emergency Management
IS-242: Effective Communication	E/L102: Science of Disasters
IS-244: Developing and Managing Volunteers	E/L103: Planning Emergency Operations
	E/L104: Exercise Design
	E/L105: Public Information & Warning

The EMI Basic Academy provides this foundational Emergency Management education. To ensure the professional development of the emergency management workforce, the recipients must ensure a routine capabilities assessment is accomplished and an IPP is developed and implemented.

12.8.5. TRAINING AND EXERCISE REPORTING

- All EMPG Program-funded exercise and training activities must be captured in the approved EMPG Program Work Plan and should be included in the IPP. This includes training for which the

[3] NIMS training courses IS-100, IS-200, IS-700, and IS-800 only need to be taken once to fulfill requirements. Also, previous versions of the IS courses are still considered as meeting the NIMS training requirement.

[4] Generally, any course version and any delivery method (Resident (E), Local (L), Virtual (K) will satisfy the NIMS training requirements. See NDEMU | EMPP | National Emergency Management Basic Academy for additional details on Basic Academy prerequisites and courses and Emergency Management Institute - Independent Study (IS) | Course List for details on available Independent Study courses.

only expenses are for overtime and/or backfill costs associated with emergency management personnel attending the training.

- EMPG Program-funded exercise costs in the Work Plan can include costs to plan, conduct and evaluate the exercise (e.g., planning, materials, props, contractual services for conducting the exercise, AAR, and IP, etc.).

- All EMPG Program-funded training activities must be reported quarterly. To simplify reporting, it is recommended the recipient submit an updated Training Data Table from the EMPG Program Work Plan Template as an attachment to the quarterly PPR. For those recipients who choose not to use the EMPG Program Work Plan Template, the data and information found in the Training Data Table must still be submitted (in any chosen format) as an attachment to the PPR.

- EMPG Program-funded personnel costs associated with exercises are not required in the EMPG Program Work Plan Template for application or reporting purposes.

- Recipients are encouraged to enter their exercise information into the Preparedness Toolkit.

- Recipients must have a current multi-year IPP that identifies preparedness priorities and activities. The current multi-year IPP must be submitted to hseep@fema.dhs.gov and the Regional EMPG Program Manager and indicate which fiscal year's funds were used (if applicable) before Jan. 31 of each year.

- AAR/IPPs must be submitted to the Regional EMPG Program Manager within 90 days following completing the the single exercise or progressive series. The Regional Program Manager will ensure that copies of AARs/IPPs are sent to hseep@fema.dhs.gov.

    - Recipients are encouraged to submit AAR/IPs reflecting tabletop exercises that validate critical plans or those reflecting large-scale functional or full-scale exercises that took place at the state, territorial, tribal, or regional level. Recipients are discouraged from submitting AAR/IPs specific to local jurisdictions that reflect drills.

    - If a state, territory, Tribal Nation, or local jurisdiction has experienced a major disaster and they would like to request exemptions for a scheduled exercise, the recipient should send this request to its assigned Regional EMPG Program Manager through the quarterly PPR. Exemptions will be reviewed by the Region on a case-by-case basis.

- Recipients can access a sample AAR/IP template at the Improvement Planning Templates page on Preparedness Toolkit.

- Recipients must report their NIMS implementation status of their jurisdiction and sub-jurisdictions, including the training of personnel, in the applicable secondary NIMS assessment portion of the URT as part of their THIRA/SPR submission.

- Recipients must maintain proof of completion of training requirements. Recipients are encouraged to use the OneResponder system to enter, track, and report training.

- Training Information Reporting System ("Web Forms"): Web Forms is an electronic data management system built to assist SAA TPOCs and federal agencies to submit **non-NTED training courses** for inclusion in the State/Federal-Sponsored Course Catalog. The information collected is used in a two-step review process to ensure that the training programs adhere to the EMPG Program's intent, and the course content is sound and current. While reporting training activities

through Web Forms is not required under the EMPG Program, the system remains available and can be accessed through the Web-Forms section of the FEMA National Preparedness Course Catalog to support recipients in their own tracking of training deliveries.

12.9. Reviewing and Updating Planning Products

Based on the applicant's current THIRA/SPR, capability levels, and resources, plans should be reviewed on an annual basis to determine if they remain relevant or need to be updated. This review should be based on a current THIRA/SPR and utilize information gathered during the capability validation process. These reviews will provide a means to determine priorities, direct preparedness actions, and calibrate goals and objectives.

12.10. Program Performance Reporting Requirements

12.10.1. STANDARDIZED PROGRAMMATIC REPORTING FOR THE EMERGENCY MANAGEMENT PERFORMANCE GRANT PROGRAM

The EMPG Program Work Plan Template standardizes data collection, which enables improved analysis and reporting. The EMPG Program Work Plan includes 10 components:

1. Grant Investment Strategy
2. Grant Activities Outline
3. Detailed Budget – Excluding M&A
4. Budget Narrative – Excluding M&A
5. Detailed Budget – M&A Only
6. Budget Narrative – M&A Only
7. EMPG Program Summary
8. Implementation Schedule
9. Training Data Table
10. Exercise Data Table

Although using the fiscal years"s EMPG Program Work Plan Template is not mandatory (see the EMPG Program Work Plan template in the EMPG Program NOFO), baseline data on personnel, training, and exercises, as well as the information included on the Grant Activities Outline and Implementation Schedule, must be provided in the EMPG Program Work Plan at the time of application regardless of the chosen work plan format.

The status of all EMPG Program-funded plans, training, and exercise activities, any risks that may affect project progress or success, and updates to project schedules, must be reported quarterly as part of the PPR. To facilitate reporting, recipients are encouraged to submit an updated Implementation Schedule, Training Data Table, and Exercise Data Table from the EMPG Program Work Plan Template as an attachment to the quarterly PPR. Recipients who choose not to use the

EMPG Program Work Plan Template must still provide the updated data and information included in the Implementation Schedule, Training Data Table, and Exercise Data Table, but may use a different format for reporting that information in their PPR submission.

13. Abbreviations and Acronyms

Abbreviation	Definition
AAR	After-Action Report
ABA	Architectural Barriers Act of 1968
ADA	Americans with Disabilities Act
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
AEL	Authorized Equipment List
AHJ	Authority Having Jurisdiction
AMSC	Area Maritime Security Committees
AMSP	Area Maritime Security Plan
ANSI	American National Standards Institute
AOR	Authorized Organization Representative
ASPR	Assistant Secretary for Preparedness and Response
ATF	Alcohol, Tabaco, Firearms, and Explosives
BABAA	Build America, Buy America Act
BASE	Baseline Assessment for Security Enhancement
BCRTP	Business Continuity and Resumption of Trade Plans
BPETS	Border Patrol Enforcement Tracking System
BSIR	Biannual Strategy Implementation Report
CAD	Computer Assisted/Aided Dispatch
CAP	Corrective Action Plans
CART	Computer Aided Real-Time Translation
CBP	Customs and Border Protection
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CDC	Centers for Disease Control and Prevention
CDP	Center for Domestic Preparedness
CGC	Continuity Guidance Circular

Abbreviation	Definition
CISA	Cybersecurity and Infrastructure Security Agency
COAM	Customer-Owned and Managed
COMU	Communications Unit
COTP	Captain of the Port
CPG	Comprehensive Preparedness Guide
CSPs	Commercial Service Providers
CTG	Continuing Training Grants
CWMD	Countering Weapons of Mass Destruction
CY	Calendar Year
DAR	Daily Activity Report
DEC	Disaster Emergency Communications
DHS	Department of Homeland Security
DM	Distribution Management
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
ECS	Enhanced Cybersecurity Services
EDCT	Explosives Detection Canine Team
EHP	Environmental Planning and Historic Preservation
EMA	Emergency Management Agency
EMAC	Emergency Management Assistance Compact
EMAP	Emergency Management Accreditation Program
EMI	Emergency Management Institute
EMM	Enterprise Mobility Management
EMP	Electromagnetic Pulse
EMPG	Emergency Management Performance Grant
EMPP	Emergency Management Professional Program

Abbreviation	Definition
EMS	Emergency Medical Services
EMSC	Emergency Medica Services for Children
EO	Executive Order
EOP	Emergency Operations Plan
EPC	Evolved Packet Core
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FEMA GO	FEMA Grants Outcomes
FFR	Federal Financial Report
FFRMS	Federal Flood Risk Management Standard
FirstNet	First Responder Network
FLR	First Line Review
FNARS	FEMA National Radio System
FRAGO	Fragmentary Order
FRTS	First Responder Training System
FSP	Facility Security Plan
FVA	Freeboard Value Approach
FY	Fiscal Year
GAAP	General Accepted Accounting Principles
GAO	Government Accountability Office
GFI	Government Furnished Information
GIS	Geographic Information Systems
GPD	Grant Programs Directorate
GSA	General Services Administration
HHS	Health and Human Services

Abbreviation	Definition
HIDTA	High-Intensity Drug Trafficking Areas
HPP	Hospital Preparedness Program
HSA	Homeland Security Act of 2002
HSEEP	Homeland Security Exercise and Evaluation Program
HSGP	Homeland Security Grant Program
HSIN	Homeland Security Information Network
I&A	Intelligence and Analysis
IAPPG	Individual Assistance Program and Policy Guide
IB	Information Bulletin
IBSGP	Intercity Bus Security Grant Program
IEDDA	International Explosive Detection Dog Association
IGSA	Inter-Governmental Service Agreement
IJ	Investment Justification
IL	Interagency Logistics
INA	Immigration and Nationality Act
IOC	Interagency Operations Centers
IP	Improvement Plan
IPAWS	Integrated Public Alert and Warning System
IPP	Integrated Preparedness Plan
IPPWs	Integrated Preparedness Planning Workshops
IPR	Intercity Passenger Rail
IPT	Integrated Planning Team
IRPF	Infrastructure Resilience Planning Framework
ISE	Information Sharing Environment
IT	Information Technology
JES	Joint Explanatory Statement
K-9	Canines

Abbreviation	Definition
LCAT2	Logistics Capability Tool 2
LESO	Law Enforcement Support Office
LTE	Long-Term Evolution
M&A	Management and Administration
MCOV	Mobile Communications Office Vehicles
MDA	Maritime Domain Awareness
MDM	Mobile Device Management
MERS	Mobile Emergency Response Support
MSAs	Metropolitan Statistical Areas
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act
NCPC	National Cybersecurity Preparedness Consortium
NCSWIC	National Council of Statewide Interoperability Coordinators
ND	Non-Disaster
NDAA	National Defense Authorization Act
NDEMU	National Disaster and Emergency Management University
NDPC	National Domestic Preparedness Consortium
NECP	National Emergency Communications Plan
NEDCTP	National Explosives Detection Canine Team Program
NEP	National Exercise Program
NGO	Nongovernmental Organization
NHTSA	National Highway Traffic Safety Administration
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
NPCA	National Police Canine Association

Abbreviation	Definition
NPD	National Preparedness Directorate
NQS	National Qualification System
NRF	National Response Framework
NSGP	Nonprofit Security Grant Program
NSI	Nationwide Suspicious Activity Reporting Initiative
NSSE	National Security Special Event
NTED	National Training and Education Division
NTIA	National Telecommunications and Information Administration
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONCP	Office of National Continuity Programs
OPSG	Operation Stonegarden
PAPPG	Public Assistance Program and Policy Guide
PARS	Payment and Reporting Systems
PDAT	Procurement Disaster Assistance Team
PHEP	Public Health Emergency Preparedness
POC	Point of Contact
PODs	Points of Distribution
POP	Period of Performance
PPD	Presidential Policy Directive
PPE	Personal Protective Equipment
PPR	Performance Progress Report
PRICE Act	Personal Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act
PRMP	Port Wide Risk Mitigation Plan
PSGP	Port Security Grant Program
PUGPG	Procurement Under Grants Policy Guide
PTT	Push-to-Talk

Abbreviation	Definition
RANs	Radio Access Networks
RDPC	Rural Domestic Preparedness Consortium
RECC	Regional Emergency Communications Coordinator
RECCWG	Regional Emergency Communications Coordination Working Groups
RECP	Regional Emergency Communications Plan
RF	Radio Frequency
RFI	Request for Information
RISS	Regional Information Sharing Systems
RMS	Records Management Systems
R/Q	Responsibility/Qualification
RRAP	Regional Resilience Assessment Program
RTSWGs	Regional Transportation Security Working Groups
SA	Signatory Authority
SAA	State Administrative Agency
SAC	Senior Advisory Committee
SAR	Suspicious Activity Report
SAT	Simplified Acquisition Threshold
SCIP	Statewide Communication Interoperability Plan
SDRC	State Disaster Recovery Coordinator
SEFA	Schedule of Expenditures of Federal Awards
SHSP	State Homeland Security Program
SIEC	Statewide Interoperability Executive Committee
SIGB	Statewide Interoperability Governance Board
SIMS	Subscriber Identification Modules
SLDHTF	State-Led Disaster Housing Task Force
SLTT	State, Local, Tribal, and Territorial
SOP	Standard Operating Procedure

Abbreviation	Definition
SPF	Single Point of Failure
SPOC	Single Point of Contact
SPR	Stakeholder Preparedness Review
sUAS	Small Unmanned Aircraft Systems
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
the Goal	National Preparedness Goal
THIRA	Threat and Hazard Identification and Risk Assessment
THSGP	Tribal Homeland Security Grant Program
TICP	Tactical Interoperability Communications Plan
TISB	Transportation Infrastructure Security Branch
TPOC	Training Point of Contact
TPP	Training Partner Program
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSGP	Transit Security Grant Program
TSI	Transportation Security Inspector
UAS	Unmanned Aircraft System
UASI	Urban Area Security Initiative
UAWG	Urban Area Working Group
UICC	Universal Integrated Circuit Cards
URT	Unified Reporting Tool
USB	Universal Serial Bus
USBP	United States Border Patrol
USCG	United States Coast Guard
USPCA	U.S. Police Canine Association
USSS	United States Secret Service

Abbreviation	Definition
VASP	Vulnerability Assessment and Security Plan
VPN	Virtual Private Network
VSP	Vessel Security Plan