



FEMA Preparedness Grants Manual

FEMA Grant Programs Directorate

February 2020



FEMA

Table of Contents

Table of Contents	2
About the Federal Emergency Management Agency (FEMA)	7
Overview of FEMA	7
Overview of Preparedness Grant Programs	7
<i>Homeland Security Grant Program (HSGP)</i>	7
<i>Tribal Homeland Security Grant Program (THSGP)</i>	8
<i>Nonprofit Security Grant Program (NSGP)</i>	8
<i>Transit Security Grant Program (TSGP)</i>	8
<i>Intercity Bus Security Grant Program (IBSGP)</i>	8
<i>Intercity Passenger Rail (IPR) Program – Amtrak</i>	8
<i>Port Security Grant Program (PSGP)</i>	8
<i>Emergency Management Performance Grant (EMPG)</i>	8
Foreword	9
The National Preparedness Goal	9
Pre-Award Application and Submission	10
Pre-Submission Information	10
<i>Agreeing to Terms and Conditions of the Award</i>	10
<i>Address to Request Application Package</i>	11
<i>Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application</i>	11
<i>Electronic Delivery</i>	12
<i>How to Register to Apply through Grants.gov</i>	12
<i>How to Submit an Initial Application to DHS/FEMA via Grants.gov</i>	14
<i>Submitting the Final Application in Non-Disaster Grants System (ND Grants)</i>	15
<i>Timely Receipt Requirements and Proof of Timely Submission</i>	15
<i>Content and Form of Application Submission</i>	15
<i>Intergovernmental Review</i>	16
<i>Funding Restrictions and Allowable Costs</i>	16
Award Determination and Obligation	19
Allocations	19
<i>Risk Methodology</i>	19
<i>Application Evaluation Criteria</i>	19
<i>Supplemental Financial Integrity Review</i>	20
<i>Review and Selection Process</i>	20
Federal Award Administration Information	20
<i>Notice of Award</i>	20
<i>Pass-Through Requirements</i>	21

<i>Administrative and National Policy Requirements</i>	21
Post-Award Management and Implementation	24
Reporting	24
Federal Financial Reporting Requirements	24
<i>Federal Financial Report (FFR)</i>	24
<i>Financial Reporting Periods and Due Dates</i>	24
Program Performance Reporting Requirements	24
<i>Performance Progress Report (PPR)</i>	24
<i>Program Performance Reporting Periods and Due Dates</i>	25
Additional Programmatic Reporting Requirements and Information	25
<i>Biannual Strategy Implementation Report (BSIR)</i>	25
Closeout Reporting Requirements	25
Administrative Closeout	26
Disclosing Information per 2 C.F.R. § 180.335	26
Reporting of Matters Related to Recipient Integrity and Performance	27
<i>Single Audit Report</i>	27
Additional Information	28
Monitoring and Oversight	28
<i>Overview</i>	28
<i>Financial Monitoring</i>	29
<i>Programmatic Monitoring Overview and Approach</i>	31
Case Studies and Use of Grant-Funded Resources During Real-World Incident Operations	32
Conflicts of Interest in the Administration of Federal Awards or Subawards	32
Period of Performance (POP) Extensions	33
Procurement Integrity	33
<i>Competition and Conflicts of Interest</i>	34
<i>Supply Schedules and Purchasing Programs</i>	35
<i>Record Retention</i>	36
Actions to Address Noncompliance	37
Audits	38
Disability and Limited English Proficiency Integration	39
National Campaigns and Programs	41
Whole Community Preparedness	41
Active Shooter Preparedness	41
Soft Targets and Crowded Places	42
Community Lifelines	42
Program Appendix A: Homeland Security Grant Program (HSGP)	A-1
Alignment of HSGP to the National Preparedness System	A-1
Reporting on the Implementation of the National Preparedness System	A-2
<i>Identifying and Assessing Risk and Estimating Capability Requirements</i>	A-2
<i>Building and Sustaining Capabilities</i>	A-2
<i>NIMS Implementation</i>	A-2

<i>Planning to Deliver Capabilities</i>	A-3
<i>Validating Capabilities</i>	A-3
Fusion Centers	A-4
Continuity of Operations	A-6
Governance	A-7
Supplemental SHSP and UASI Guidance	A-11
Supplemental Operation Stonegarden Grant (OPSG) Program Guidance	A-13
OPSG Operational Guidance	A-31
HSGP Supplemental Material	A-37
Fusion Center Performance Measures	A-39
Supplemental Emergency Communications Guidance	A-41
Program Appendix B: Tribal Homeland Security Grant Program (THSGP)	B-1
Alignment of THSGP to the National Preparedness System	B-1
THSGP Funding Guidelines	B-4
THSGP Priorities	B-4
Allowable Costs	B-4
THSGP Investment Modifications – Changes in Scope or Objective	B-11
Program Appendix C: Nonprofit Security Grant Program (NSGP)	C-1
NSGP Funding Guidelines	C-1
NSGP Priorities	C-1
Allowable Costs	C-1
NSGP Investment Modifications – Changes in Scope or Objective	C-5
Pass-Through Requirements	C-5
DUNS/SAM Requirements for Recipients and Subrecipients	C-6
Program Appendix D: Transit Security Grant Program (TSGP)	D-1
Applicable Regulations	D-1
Pre-Award Costs	D-1
TSGP Priorities	D-1
Allowable Direct Costs	D-1
Allowable Indirect Costs	D-11
Unallowable Costs	D-11
Maintenance and Sustainment Costs	D-11
Encouraged Use of Certain Products Produced in the United States	D-11
Program Appendix E: Intercity Bus Security Grant Program (IBSGP)	E-1
IBSGP Priorities	E-1
Pre-Award Costs	E-1
Allowable Direct Costs	E-1
Indirect Costs (Facilities and Administration [F&A])	E-7
Unallowable Costs	E-7
Other Allowable Costs	E-8
Encouraged Use of Certain Products Produced in the United States	E-9

Program Appendix F: Intercity Passenger Rail (IPR) Program **F-1**

Applicable Regulations	F-1
IPR Priorities	F-1
Allowable Costs	F-1
Operational Activities	F-2
Funding Availability for OPacks	F-3
Specific Guidance on Explosive Detection Canine Teams (EDCT)	F-5
EDCT Submission Requirements	F-5
Requirements for Small Unmanned Aircraft Systems	F-6
Cybersecurity Projects	F-7
Capital (Construction) Projects Guidance	F-7
Training and Awareness Campaigns	F-8
Management and Administration (M&A)	F-10
Indirect Costs	F-11
Unallowable Costs	F-11
Maintenance and Sustainment Costs	F-11
Encouraged Use of Certain Products Produced in the United States	F-11

Program Appendix G: Port Security Grant Program (PSGP) **G-1**

Applicable Regulations	G-1
PSGP Priorities	G-1
Limitations on Funding	G-1
Allowable Direct Costs	G-1
Allowable Indirect Costs	G-12
Unallowable Costs	G-12
Maintenance and Sustainment Costs	G-13
Port-Wide Risk Management Plans	G-14
Sample Memorandum of Understanding/Agreement	G-14

Program Appendix H: Emergency Management Performance Grant Program **H-1**

Alignment of EMPG to the National Preparedness System	H-1
Reporting on the Implementation of the National Preparedness System	H-1
Logistics Planning	H-2
Evacuation Planning	H-3
Disaster Housing Planning	H-4
State-Led Disaster Housing Task Force	H-4
Disaster Financial Management Policies and Procedures	H-6
Additional Considerations	H-9
Program Performance Reporting Requirements	H-10

EMPG Funding Guidelines **H-12**

Allowable Costs	H-12
Planning	H-12
Continuity Planning	H-14
Organization	H-14
Equipment	H-15

Training	H-16
Exercises	H-19
Maintenance and Sustainment	H-20
Unallowable Costs	H-21
EMPG Work Plan	H-22

About the Federal Emergency Management Agency (FEMA)

Overview of FEMA

For more than 40 years, FEMA has helped people before, during, and after disasters. FEMA remains committed to building and developing a culture of preparedness across the country and unifying all levels of community and government into an integrated approach to emergency management. FEMA is part of a larger team of federal agencies, state, local, tribal, and territorial (SLTT) governments, and non-governmental partners that share responsibility for emergency management and national preparedness. Those closest to impacted areas are the true first responders during any emergency or disaster—individuals, families, neighbors, and local communities. FEMA’s role is to coordinate Federal resources to supplement SLTT capabilities. FEMA does this by coordinating through the levels of government, meaning that states and their local political subdivisions, tribes, and territories are our primary partners.

Overview of Preparedness Grant Programs

FEMA has the statutory authority to deliver numerous disaster and non-disaster financial assistance programs in support of FEMA’s mission, largely through grants and cooperative agreements. These programs account for a significant amount of the Federal 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 circulars, and Federal appropriations law principles. FEMA has developed this Manual to provide additional direction on grant policy and implementation for the following grant programs:

[Homeland Security Grant Program \(HSGP\)](#)

The HSGP includes a suite of risk-based grants to assist 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 state, local, tribal, and territorial 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)*
UASI assists high-threat, high-density 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 Customs and Border Protection (CBP), United States Border Patrol (USBP), and federal, state, local, tribal, and territorial 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 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. State, local, tribal, and territorial (SLTT) law enforcement agencies utilize their own law enforcement authorities to support the border security mission and do not receive any additional authority as a result of participation in OPSG.

[Tribal Homeland Security Grant Program \(THSGP\)](#)

The THSGP provides funding directly to eligible tribes to strengthen their capacities to prevent, prepare for, protect against, and respond to potential terrorist attacks.

[Nonprofit Security Grant Program \(NSGP\)](#)

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

[Transit Security Grant Program \(TSGP\)](#)

The 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.

[Intercity Bus Security Grant Program \(IBSGP\)](#)

The IBSGP provides funds to eligible private operators of intercity over-the-road bus transportation systems to protect critical transportation infrastructure and travelling public from acts of terrorism, and to increase transportation infrastructure resilience.

[Intercity Passenger Rail \(IPR\) Program – Amtrak](#)

The IPR 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.

[Port Security Grant Program \(PSGP\)](#)

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

[Emergency Management Performance Grant \(EMPG\)](#)

The FY 2020 EMPG program will provide funds to assist state, local, tribal, and territorial emergency management agencies in obtaining the resources required for implementation of the National Preparedness System and the National Preparedness Goal (the Goal) of a secure and resilient nation.

Foreword

FEMA has developed this **Preparedness Grants Manual** to guide applicants and grant recipients on how to manage their grants and other resources. Recipients seeking guidance on policies and procedures for managing preparedness grants should reference this manual for further information on both program-specific information as well as overall guidance on rules and regulations that guide the proper management of FEMA grants.

The 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.” See Dep’t of Homeland Sec., *National Preparedness Goal, Second Edition*, 1 (Sept. 2015). 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 [National Preparedness Goal](#) describes the five mission areas as follows:

- **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.” *Id.* at A-2.

For more information about the National Preparedness Goal, go to <https://www.fema.gov/national-preparedness-goal>. 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 information on the National Preparedness System is available at <http://www.fema.gov/national-preparedness-system>. Additional details regarding the National Preparedness System and how it is supported by these grant programs can be found in the program-specific appendices.

Pre-Award Application and Submission

Pre-Submission Information

These instructions apply to the following programs:

- Homeland Security Grant Program¹
- Tribal Homeland Security Grant Program
- Nonprofit Security Grant Program
- Transit Security Grant Program
- Intercity Bus Security Grant Program
- Intercity Passenger Rail Program
- Port Security Grant Program
- Emergency Management Performance Grant Program

All applications **must** be received by the established deadline. The Non-Disaster (ND) Grants System has a date stamp that indicates when an application is submitted. Applicants will receive an electronic message confirming receipt of their submission. For additional information on how an applicant will be notified of application receipt, see the section titled “Timely Receipt Requirements and Proof of Timely Submission.”

DHS/FEMA will not review applications that are received after the deadline or consider them for funding. DHS/FEMA may, however, extend the application deadline on request for an applicant who can demonstrate that good cause exists to justify extending the deadline. Good cause for an extension may include technical problems outside of the applicant’s control that prevent submission of the application by the deadline, other exigent or emergency circumstances, or statutory requirements for DHS/FEMA to make an award.

Applicants experiencing technical problems outside of their control must notify the respective FEMA Program Analyst as soon as possible and before the application deadline. Failure to timely notify FEMA of the issue that prevented the timely filing of the application may preclude consideration of the award. “Timely notification” of FEMA means the following: prior to the application deadline and within 48 hours after the applicant became aware of the issue.

For additional assistance using the ND Grants System, please contact the ND Grants Service Desk at (800) 865-4076 or NDGrants@fema.dhs.gov. The ND Grants Service Desk is available Monday through Friday, 9:00 a.m. – 6:00 p.m. ET. If applicants do not know their FEMA Program Analyst or if there are programmatic questions or concerns, please contact the Centralized Scheduling and Information Desk (CSID) by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

Agreeing to Terms and Conditions of the Award

By submitting an application, the applicant agrees to comply with the requirements of the applicable NOFO, this Manual, and the applicable appendix to this Manual, as well as the terms and conditions of its award should it receive an award.

¹ Under this program, these instructions also apply to SHSP, UASI, and OPSG.

Address to Request Application Package

Initial applications are processed through the [Grants.gov](https://www.grants.gov) portal. Final applications are completed and submitted through FEMA’s Non-Disaster Grants (ND Grants) System. Application forms and instructions are available on [Grants.gov](https://www.grants.gov), and hard copies of the NOFO and associated application materials are not available. To access these materials, go to <http://www.grants.gov>, select “Applicants” then “Apply for Grants.” In order to obtain the application package, select “Download a Grant Application Package.” Enter the Assistance Listings (formerly CFDA) and/or the funding opportunity number located on the cover of this NOFO, select “Download Package,” and then follow the prompts to download the application package. In addition, the following Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice and all relevant NOFOs is (800) 462-7585.

Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application

Applying for an award under the programs covered by this Manual is a multi-step process. To ensure that their applications are submitted on time, applicants are advised to start the required steps well in advance of their application submissions. Failure of an applicant to comply with any of the required steps before the deadline for submitting an application may disqualify that application from funding.

In order to apply for an award, all applicants must:

1. Apply for, update, or verify their Data Universal Numbering System (DUNS) number from Dun & Bradstreet and Employer Identification Number from the Internal Revenue Service;
2. In the application, provide a valid DUNS number, which is currently the unique entity identifier;
3. Have an account with login.gov;
4. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
5. Create a Grants.gov account;
6. Add a profile to a Grants.gov account;
7. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
8. Register in ND Grants;
9. Submit an initial application in Grants.gov;
10. **Submit the final application in ND Grants, including electronically signing applicable forms;** and
11. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency.

Specific instructions on how to apply for, update, or verify a DUNS number or SAM registration or establish an AOR are included below in the steps for applying through Grants.gov. Applicants are advised that DHS/FEMA may not make a federal award until the applicant has complied with all applicable DUNS and SAM requirements. Therefore, an applicant’s SAM registration must be active not only at the time of application, but also during the application review period and when DHS/FEMA is ready to make a federal award. Further, as noted above, an applicant’s or recipient’s SAM registration must remain active for the duration of an active federal award. If an applicant’s SAM registration is expired at the time of application, expires during application review, or expires any other time before award, DHS/FEMA may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

Electronic Delivery

DHS/FEMA is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS/FEMA requires applicants to submit their initial applications online through Grants.gov and to submit their final applications through ND Grants.

How to Register to Apply through Grants.gov

1. **Instructions:** Registering and applying for an award under this program is a multi-step process and requires time to complete. Read the instructions below about registering to apply for DHS/FEMA funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration process will alleviate last-minute searches for required information.

The registration process can take up to four weeks to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required application submission deadlines.

Organizations must have a Data Universal Numbering System (DUNS) Number and an active System for Award Management (SAM) registration.

Organizations must also have a Grants.gov account to apply for an award under this program.

In order to apply through Grants.gov, organizations must have a DUNS Number, an active SAM registration, and a Grants.gov account to apply for grants.

If individual applicants are eligible to apply for a grant funding opportunity, refer to <https://www.grants.gov/web/grants/applicants/registration.html>.

Organization applicants can find complete instructions here: <https://www.grants.gov/web/grants/applicants/organization-registration.html>.

2. **Obtain a DUNS Number:** All entities applying for funding, including renewal funding, must have a DUNS number from Dun & Bradstreet (D&B). Applicants must enter the DUNS number in the data entry field labeled "Organizational DUNS" on the SF-424 form.

For more detailed instructions for obtaining a DUNS number, refer to <https://www.grants.gov/web/grants/applicants/organization-registration/step-1-obtain-duns-number.html>.

3. **Obtain Employer Identification Number:** In addition to having a DUNS number, all entities applying for funding must provide an employer Identification Number (EIN). The EIN can be obtained from the IRS by visiting: <https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online>.
4. **Create a login.gov account:** Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account here: https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd3.

Applicants only have to create a login.gov account once. For applicants that are existing SAM users, use the same email address for the login.gov account as with SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to:
<https://www.sam.gov/SAM/pages/public/loginFAQ.jsf>.

5. **Register with SAM:** In addition to having a DUNS number, all organizations applying online through Grants.gov must register with SAM. Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually.

For more detailed instructions for registering with SAM, refer to
<https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html>.

6. **Create a Grants.gov Account:** The next step in the registration process is to create an account with Grants.gov. Applicants must know their or their organization's DUNS number to complete this process.

For more information, follow the on-screen instructions or refer to
<https://www.grants.gov/web/grants/applicants/registration.html>.

7. **Add a Profile to a Grants.gov Account:** A profile in Grants.gov corresponds to a single applicant organization the user represents or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to a single Grants.gov account to access all of your grant applications. To add an organizational profile to your Grants.gov account, enter the DUNS Number for the organization in the DUNS field while adding a profile.

For more detailed instructions about creating a profile on Grants.gov, refer to
<https://www.grants.gov/web/grants/applicants/registration/add-profile.html>.

8. **EBiz POC Authorized Profile Roles:** After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access are sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the AOR role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role.

For more detailed instructions about creating a profile on Grants.gov, refer to
<https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html>.

9. **Track Role Status:** To track your role request, refer to
<https://www.grants.gov/web/grants/applicants/registration/track-role-status.html>.

10. **Electronic Signature:** When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted into the signature line of the application, serving as the electronic signature. The EBiz POC must authorize individuals who are able to make legally binding commitments on behalf of the organization as an AOR. Please ensure you have been authorized by the EBiz POC as this step is often missed, and it is crucial for valid and timely submissions.



How to Submit an Initial Application to DHS/FEMA via Grants.gov

Grants.gov applicants apply online using a workspace. A workspace is a shared, online environment where members of a grant team may simultaneously access and edit different web forms within an application. For each Notice of Funding Opportunity (NOFO), you can create individual instances of a workspace. Applicants are encouraged to submit their initial applications in [Grants.gov](#) at least seven days before the application deadline.

In Grants.gov, applicants need to submit the following forms:

- SF-424, Application for Federal Assistance
- Grants.gov Lobbying Form, Certification Regarding Lobbying

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using a workspace, refer to: <https://www.grants.gov/web/grants/applicants/workspace-overview.html>

1. **Create a Workspace:** Creating a workspace allows you to complete it online and route it through your organization for review before submitting.
2. **Complete a Workspace:** Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission.
3. **Adobe Reader:** If you decide not to apply by filling out web forms, you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS/FEMA forms. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, and then accessed through Adobe Reader.

NOTE: Visit the Adobe Software Compatibility page on [Grants.gov](#) to download the appropriate version of the software at <https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html>.

4. **Mandatory Fields in Forms:** In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.
5. **Complete SF-424 Fields First:** The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and DUNS number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.
6. **Submit a Workspace:** An application may be submitted through workspace by clicking the “Sign and Submit” button on the Manage Workspace page, under the Forms tab. Grants.gov recommends submitting your application package at least seven days prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.
7. **Track a Workspace:** After successfully submitting a workspace package, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the confirmation page that is generated after submission. Using the tracking number,

access the Track My Application page under the Applicants tab or the Details tab in the submitted workspace.

Additional Training and Applicant Support: For additional training resources, including video tutorials, refer to <https://www.grants.gov/web/grants/applicants/applicant-training.html>. Grants.gov provides applicants 24/7 support via the toll-free number 1-800-518-4726 and email at support@grants.gov. For questions related to a specific grant contact the number listed in the application package of the grant for which you are applying.

If you are experiencing difficulties with your submission, it is best to call the [Grants.gov](#) Support Center and get a ticket number. The Support Center ticket number will assist the DHS/FEMA with tracking your issue and understanding background information on the issue.

Submitting the Final Application in Non-Disaster Grants System (ND Grants)

After submitting the initial application in [Grants.gov](#), eligible applicants will be notified by DHS/FEMA and asked to proceed with submitting their complete application package in [ND Grants](#). Applicants can register early with ND Grants and are encouraged to begin their ND Grants registration at the time of this announcement or, at the latest, seven days before the application deadline. Early registration will allow applicants to have adequate time to start and complete their applications.

Applicants needing assistance registering for the ND Grants system should contact ndgrants@fema.dhs.gov or (800) 865-4076. For step-by-step directions on using the ND Grants system and other guides, please see <https://www.fema.gov/non-disaster-grants-management-system>.

In [ND Grants](#), applicants will be prompted to submit the standard application information required as described in the “Content and Form of Application Submission” section below. The Standard Forms are auto-generated in ND Grants, but applicants may access these forms in advance through the Forms tab under the [SF-424 family on Grants.gov](#). Applicants should review these forms before applying to ensure they have all the information required.

For program-specific application submission requirements, please refer to the applicable program NOFO and applicable appendix to this Manual.

Timely Receipt Requirements and Proof of Timely Submission

As application submission is a two-step process, the applicant with the AOR role who submitted the application in Grants.gov will receive an acknowledgement of receipt, a tracking number (GRANTXXXXXXXX) from Grants.gov, and an Agency Tracking Number (EMX-2020-XX-XXXX) with the successful transmission of its initial application. This notification does not serve as proof of timely submission, as the application is not complete until it is submitted in ND Grants.

All applications must be received in ND Grants by **5:00 PM ET** on the application deadline. Proof of timely submission is automatically recorded by ND Grants. An electronic date/time stamp is generated within the system when the application is successfully received by ND Grants. Additionally, the applicant(s) listed as contacts on the application will receive a system-generated email to confirm receipt.

Content and Form of Application Submission

Required Forms

For all programs, the following forms or information are required to be submitted in either Grants.gov or ND Grants. The Standard Forms (SFs), submitted either through Grants.gov, through forms generated in

ND Grants, or as an attachment in ND Grants, are available at <https://www.grants.gov/web/grants/forms/sf-424-family.html>.

- **SF-424, Application for Federal Assistance**, submitted through Grants.gov
- **Grants.gov Lobbying Form, Certification Regarding Lobbying**, submitted through Grants.gov
- **SF-424A, Budget Information (Non-Construction)**, submitted via the forms generated by ND Grants
 - **For construction under an award, submit: SF-424C, Budget Information (Construction)**, submitted via the forms generated by ND Grants, in addition to or instead of SF-424A
- **SF-424B, Standard Assurances (Non-Construction)**, submitted via the forms generated by ND Grants
 - **For construction under an award, submit: SF-424D, Standard Assurances (Construction)**, submitted via the forms generated by ND Grants, in addition to or instead of SF-424B
- **SF-LLL, Disclosure of Lobbying Activities**, via the forms generated by ND Grants
- **Indirect Cost Agreement**, submitted as an attachment in ND Grants if the budget includes indirect costs and the applicant is required to have an indirect cost rate agreement. If the applicant is not required to have an indirect cost rate agreement but will charge indirect costs and is required to have an indirect cost rate proposal, the applicant must provide a copy of their indirect cost rate proposal with the application. See the section below on indirect costs for more information or contact the relevant Program Analyst or Grants Management Specialist for further instructions.

Generally, applicants have to submit either the non-construction forms (i.e., SF-424A and SF-424B) or construction forms (i.e., SF-424C and SF-424D), meaning that applicants that only have construction work and do not have any non-construction work need only submit the construction forms (i.e., SF-424C and SF-424D) and not the non-construction forms (i.e., SF-424A and SF-424B), and vice versa. However, applicants who have both construction and non-construction work under this program need to submit both the construction and non-construction forms.

Intergovernmental Review

An intergovernmental review may be required. Applicants must contact their State's Single Point of Contact (SPOC) to comply with the State's process under Executive Order 12372.

See <https://www.archives.gov/Federal-register/codification/executive-order/12372.html>;
<https://www.whitehouse.gov/wp-content/uploads/2019/02/SPOC-February-2019.pdf>.

Funding Restrictions and Allowable Costs

All costs charged to awards covered by this Manual must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in this Manual, the applicable program NOFO, or the terms and conditions of the award. For more information on FEMA's implementation of 2 C.F.R. Part 200, see [Information Bulletin \(IB\) No. 400](#).

In general, the Cost Principles establish standards for the allowability of costs, provide detailed guidance on the cost accounting 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 appendix to this Manual or the program NOFO, 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. In

order 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 particular FEMA award.

Additionally, all costs charged to awards must comply with the grant program's applicable statutes, policies, NOFOs, and requirements in this Manual as well as with the terms and conditions of the 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.

As part of those requirements, grant recipients and subrecipients may only use federal funds or funds applied to a cost share for the purposes set forth in this Manual, applicable NOFOs, and the terms and conditions of the award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for other federal grants/cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. Recipients are also expected to conform, as applicable, with accepted engineering practices, established codes, standards, modeling techniques, and best practices, and participate in the development of case studies demonstrating the effective use of grant funds, as requested.

Specific investments made in support of the funding priorities discussed in the appendices to this Manual 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
8. Training

Please refer to the relevant program-specific appendix for more information on funding restrictions, funding priorities, and these categories.

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.

Prohibitions on Expending Grant or Cooperative Agreement Funds for Certain Telecommunications and Video Surveillance Services or Equipment

Effective August 13, 2020, DHS/FEMA recipients and subrecipients may not use grant funds under the programs covered by this Manual and provided in FY 2020 or previous years to:

1. Procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract to procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology of any system; or

2. Enter into contracts or extend or renew contracts with entities that use “covered telecommunications equipment or services” as a substantial or essential component of any system, or as critical technology as part of any system.

This prohibition regarding certain telecommunications and video surveillance services or equipment is mandated by section 889 of the [John S. McCain National Defense Authorization Act for Fiscal Year 2019 \(FY 2019 NDAA\)](#), Pub. L. No. 115-232 (2018). Recipients and subrecipients may use DHS/FEMA grant funding to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of this Manual, applicable appendix to this Manual, and applicable NOFO. DHS/FEMA will publish additional guidance in a subsequent Information Bulletin or similar notice.

Per section 889(f)(2)-(3) of the FY 2019 NDAA, covered telecommunications equipment or services means:

1. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
2. For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
3. Telecommunications or video surveillance services provided by such entities or using such equipment; or
4. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People’s Republic of China.

Award Determination and Obligation

Allocations

Risk Methodology

DHS/FEMA defines risk as: “potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.” See Risk Steering Committee, *DHS Risk Lexicon: 2010 Edition*, (Sept. 2010), at 27, available at <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>. The DHS/FEMA risk methodology is focused on three elements:

- **Threat:** the likelihood of an attack being attempted by an adversary
- **Vulnerability:** the likelihood that an attack is successful, given that it is attempted
- **Consequence:** the effect of an event, incident, or occurrence

Please see the applicable appendix of the Preparedness Grants Manual for each award program for specific information on the risk methodology applied for each program.

Application Evaluation Criteria

Programmatic Criteria

See the Manual appendices and relevant program NOFOs for specific information on the application criteria specific to each program.

Financial Integrity Criteria

Prior to making a federal award, FEMA is required by 31 U.S.C. § 3321 note, 41 U.S.C. § 2313, and 2 C.F.R. § 200.205 to review information available through any OMB-designated repositories of government-wide eligibility qualification or financial integrity information. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

1. Financial stability.
2. Quality of management systems and ability to meet management standards.
3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

All investments selected for recommendation will also undergo an additional risk review conducted by the DHS/FEMA Grants Management Specialist to evaluate the risk for noncompliance in carrying out the federal award. Using their subject-matter expertise, the questions the DHS/FEMA Grants Management Specialist may assess include, but are not limited to:

- Is the applicant on any exclusion lists as identified in the System for Award Management (SAM.gov)?
- If the applicant has received federal funding in the past, has the applicant performed all audits required by the Single Audit requirements under 2 C.F.R. Part 200, Subpart F?
- Has the applicant provided sufficient budget information and justification as required by the NOFO?
- Are the costs proposed by the applicant in the budget information and justification allowable and reasonable based on the criteria set forth in this Manual and the applicable appendix, NOFO, and regulations?

- Is the budget representative of the total cost of performance of the projects?
- If indirect costs are included, has the applicant provided an approved Indirect Cost Rate agreement?
- Is the applicant delinquent on any federal debt?
- Has the applicant had substandard performance in a prior award?
- Is the applicant on the Do Not Pay List?

Based on the outcome of this review, DHS/FEMA may determine that it will not make an award to an applicant that poses a risk of noncompliance. DHS/FEMA may also determine that it will make an award to an at-risk applicant, subject to additional terms and conditions as described in 2 C.F.R. § 200.207.

Supplemental Financial Integrity Review

Prior to making a federal award where the anticipated federal share will be greater than the simplified acquisition threshold, currently \$250,000 (*see FEMA Information Bulletin No. 434*, Increases and Changes to the Micro-Purchase and Simplified Acquisition Thresholds):

- DHS/FEMA is required to review and consider any information about the applicant in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the [Federal Awardee Performance and Integrity Information System](#) (FAPIIS) and is accessible through the [SAM](#) website.
- An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.
- DHS/FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants, as described in 2 C.F.R. § 200.205.

Review and Selection Process

Please see the applicable NOFO for the review and selection process for that program.

Federal Award Administration Information

Notice of Award

Before accepting the award, the AOR and recipient should carefully review the award package. The award package includes instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. Recipients must accept all conditions in the applicable program NOFO as well as this Manual, in addition to any special terms and conditions in the Notice of Award to receive an award under the applicable program.

Notification of award approval is made through the ND Grants system through an automatic electronic mail to the recipient's authorized official listed in the initial application. The award date will be the date that DHS/FEMA approves the award. The recipient should follow the directions in the notification to confirm acceptance of the award. Funds will remain on hold until the recipient accepts the award through the ND Grants system and all other conditions of the award have been satisfied or until the award is otherwise rescinded.

Recipients must accept their awards no later than 60 days from the award date. The recipient shall notify DHS/FEMA of its intent to accept and proceed with work under the award through the ND Grants system. For instructions on how to accept or decline an award in the ND Grants system, please see the

[ND Grants Recipient Training Manual](#). Failure to accept a grant award within the 60-day timeframe may result in a loss of funds.

Pass-Through Requirements

Please see the applicable NOFO and applicable appendix to this Manual for information on pass-through requirements for that program.

Administrative and National Policy Requirements

All successful applicants for all DHS/FEMA grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at:

<https://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions>.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

Environmental Planning and Historic Preservation (EHP) Compliance

As a federal agency, DHS/FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by DHS/FEMA, including grant-funded projects, comply with Federal EHP regulations, laws, and Executive Orders, as applicable.

Recipients and subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the DHS/FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by DHS/FEMA in order to determine whether the proposed project has the potential to impact environmental resources or historic properties.

In some cases, DHS/FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. The EHP review process must be completed before funds are released to carry out the proposed project; otherwise, DHS/FEMA may not be able to fund the project due to noncompliance with EHP laws, executive order, regulations, and policies.

Additionally, all recipients and subrecipients receiving funding under a program covered by this Manual are required to comply with [DHS/FEMA EHP Policy Guidance, FEMA Policy #108-023-1](#). The EHP screening form is located <https://www.fema.gov/media-library/assets/documents/90195>, and further EHP guidance can be found at <https://www.fema.gov/media-library/assets/documents/118323>.

Ensuring the Protection of Civil Rights

As the Nation works towards achieving the [National Preparedness Goal](#), it is important to continue to protect the civil rights of individuals. Recipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations. Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS/FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from DHS/FEMA. The DHS Standard Terms and Conditions include a complete list of the civil rights provisions that apply to recipients. These terms and conditions

can be found in the [DHS Standard Terms and Conditions](#). Additional information on civil rights provisions is available at <https://www.fema.gov/office-equal-rights>.

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 will evolve with technological advances and initially consist of a core network and radio access network (RAN).

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.
- 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 the Statewide Interoperability Coordinator (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 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. Information Bulletin #386 has been rescinded by prior NOFOs and remains rescinded as the technical requirements and nationwide network architecture has been developed, and FirstNet is operational. Recipients, however, 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.

National Incident Management System (NIMS) Implementation

Prior to allocation of any federal preparedness awards, recipients must ensure and maintain adoption and implementation of NIMS. The list of objectives used for progress and achievement reporting is at <https://www.fema.gov/implementation-guidance-and-reporting>.

Emergency management and incident response activities require carefully managed resources (personnel, teams, facilities, equipment, and/or supplies) to meet incident needs. 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 <https://www.fema.gov/implementation-guidance-and-reporting>. Please also see the individual program appendices in this Manual for additional requirements regarding NIMS compliance for specific programs.

FEMA developed the *NIMS Guideline for the Credentialing of Personnel* 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 routinely and to facilitate multijurisdictional coordinated responses.

Although state, local, tribal, territorial, and private sector partners (including nongovernmental organizations) are not required to credential their personnel in accordance with these guidelines, FEMA strongly encourages them to do so to leverage the federal investment in the Federal Information Processing Standards 201 infrastructure and to facilitate interoperability for personnel deployed outside their home jurisdiction.

Additional information about NIMS in general is available at <http://www.fema.gov/nims-doctrine-supporting-guides-tools>.

SAFECOM

All entities using preparedness grant funding to support emergency communications investments are required to comply with the [SAFECOM Guidance on Emergency Communications Grants \(SAFECOM Guidance\)](#). 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 National Emergency Communications Plan (NECP). Conformance with the SAFECOM Guidance helps ensure that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications.

Emergency communications investments also will be reviewed jointly by DHS/FEMA and the DHS Cybersecurity and Infrastructure Security Agency (CISA) to verify compliance with SAFECOM guidance. DHS/FEMA will coordinate directly with the recipient on any compliance concerns and will provide technical assistance as necessary to help ensure full compliance.

Post-Award Management and Implementation

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.

Federal Financial Reporting Requirements

Federal Financial Report (FFR)

Recipients must report obligations and expenditures on a quarterly basis through the FFR form (SF-425) to DHS/FEMA. Recipients may review the Federal Financial Reporting Form (FFR) (SF-425) at <https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html#sortby=1>. Recipients must file the FFR electronically using the Payment and Reporting Systems (PARS).

Financial Reporting Periods and Due Dates

An FFR must be submitted quarterly throughout the period of performance (POP), including partial calendar quarters, as well as in periods where no grant award activity occurs. Future awards and fund drawdowns may be withheld if these reports are delinquent, demonstrate a lack of progress, or are insufficient in detail.

The following reporting periods and due dates apply for the FFR:

Reporting Period	Report Due Date
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30

Program Performance Reporting Requirements

Performance Progress Report (PPR)

Recipients are responsible for providing updated performance reports on a biannual basis as an attachment in ND Grants. The PPR should include the following:

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

Note: This requirement does NOT apply to EMPG, which has different performance reporting requirements. These are described in the EMPG Program Appendix to this Manual.

Program Performance Reporting Periods and Due Dates

The following reporting periods and due dates apply for the PPR:

Reporting Period	Report Due Date
January 1 – June 30	July 30
July 1 – December 31	January 30

Additional Programmatic Reporting Requirements and Information

Biannual Strategy Implementation Report (BSIR)²

In addition to the quarterly financial and biannual performance progress reports, recipients are responsible for completing and submitting BSIRs through the [Grants Reporting Tool](#) (GRT). The BSIR is due within 30 days after the end of the reporting period (July 30 for the reporting period of January 1 through June 30 (the summer BSIR report); and January 30 for 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 (POETE). The first BSIR will be due by December 31 of each calendar year in which the grant is awarded. 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 period of performance (POP) or the liquidation period ends in the middle of a reporting period, a "regular" BSIR must be submitted with full accounting of actual project information/expenditures before a Closeout BSIR can be created/submitted. The last "regular" BSIR is required because the Closeout BSIR does NOT contain full functionality to edit any project information/expenditures. Once the last "regular" BSIR is approved by GPD, the Closeout BSIR can be created/submitted. Please contact your HQ Program Analyst for guidance on the information required for the Closeout BSIR.

Closeout Reporting Requirements

Within 90 days after the end of the POP for the prime award or after an amendment has been issued to close out an award, whichever occurs first, recipients must submit the following documentation in ND Grants:

1. The final request for payment, if applicable;
2. The final FFR (SF-425);
3. Final PPR;
4. A qualitative narrative summary of the impact of those accomplishments throughout the entire POP submitted to the respective FEMA Program Analyst; and
5. Other documents required by program guidance, NOFOs, appendices to this Manual, or terms and conditions of the award.

² BSIR requirements are only applicable to the following grant programs: HSGP (SHSP, UASI, and OPSG), THSGP, EMPG, and NSGP.

In addition, any recipient that issues subawards to any subrecipient is responsible for closing out those subawards as described in 2 C.F.R. § 200.343. Recipients must ensure that they complete the closeout of their subawards in time to submit all necessary documentation and information to DHS/FEMA during the closeout of their prime award.

After the prime award closeout reports have been reviewed and approved by DHS/FEMA, a closeout notice will be completed. The notice will indicate the POP as closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the award records for at least three years from the date of the final FFR. The record retention period may be longer than three years due to an audit, litigation, or other circumstances outlined in 2 C.F.R. § 200.333.

Recipients are responsible for refunding to FEMA any unobligated balances that FEMA paid that are not authorized to be retained per 2 C.F.R. § 200.343(d).

Administrative Closeout

Administrative closeout is a mechanism for FEMA to unilaterally move forward with closeout of an award using available award information in lieu of final reports from the recipient. It is a last resort available to FEMA, and **if FEMA needs to administratively close an award, this may negatively impact a recipient's ability to obtain future funding**. This mechanism can also require FEMA to make cash or cost adjustments and ineligible cost determinations based on the information it has, which may result in identifying a debt owed to FEMA by the recipient.

FEMA may use the administrative closeout process when a recipient is not responsive to FEMA's reasonable efforts to collect required reports needed to complete the standard closeout process. FEMA will make three written attempts to collect required reports before initiating administrative closeout.

If FEMA administratively closes an award where no final FFR has been submitted, FEMA uses that administrative closeout date in lieu of the final FFR submission date as the start of the three-year record retention period under 2 C.F.R. § 200.333.

In addition, if an award is administratively closed, FEMA may decide to impose remedies for noncompliance per 2 C.F.R. § 200.338, consider this information in reviewing future award applications, or apply special conditions to existing or future awards.

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

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a recipient enters into a grant award with FEMA, the recipient must notify FEMA if it knows if it or any of the recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335:

- Are presently excluded or disqualified;
- Have been convicted within the preceding three years of any of the offenses listed in 2 C.F.R. § 180.800(a) or had a civil judgment rendered against it or any of the recipient's principals for one of those offenses within that time period;
- Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses listed in 2 C.F.R. § 180.800(a); or
- Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

At any time after accepting the award, if the recipient learns that it or any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the recipient must provide immediate written notice to FEMA in accordance with 2 C.F.R. § 180.350.

Reporting of Matters Related to Recipient Integrity and Performance

Per 2 C.F.R. Part 200, Appendix I § F.3, the additional post-award reporting requirements in 2 C.F.R. Part 200, Appendix XII may apply to applicants who, if upon becoming recipients, have a total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies that exceeds \$10,000,000 for any period of time during the period of performance of an award under this funding opportunity.

Recipients that meet these criteria must maintain current information reported in FAPIIS about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII at the reporting frequency described in paragraph 4 of Appendix XII.

Single Audit Report

For fiscal years beginning on or after December 26, 2014, recipients that expend \$750,000.00 or more from all federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report, also known as a “single audit” report.

The audit must be performed in accordance with the requirements of Government and Accountability Office’s (GAO) Government Auditing Standards, located at <https://www.gao.gov/yellowbook/overview>, and the requirements of Subpart F of 2 C.F.R. Part 200, located at <http://www.ecfr.gov/cgi-bin/text-idx?node=sp2.1.200.f>.

Additional Information

Monitoring and Oversight

Overview

Per 2 C.F.R. § 200.336, 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 review award progress and to provide any required technical assistance. 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 towards 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 towards grant goals and proactively target and address issues that may threaten grant success during the period of performance.

FEMA staff will monitor recipients periodically 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 technical assistance, 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. § 200.331. 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.

Recipient and subrecipient responsibilities also 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.

Financial Monitoring

DHS/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 helps 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 (GMSs) 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 technical assistance and recipient training; and debt collection.

In addition to the monitoring guidance outlined above, section 2022 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.).

The following preparedness grant programs are subject to HSA monitoring requirements:

- Emergency Management Performance Grant Program
- Homeland Security Grant Program
 - Operation Stonegarden Grant Program
 - State Homeland Security Grant Program
 - Urban Area Security Initiative
- Nonprofit Security Grant Program
- Transit Security Grant Program
- Port Security Grant Program

Standard Monitoring Activity: Cash Analysis

Through cash analysis, a GMS assesses and reports on the recipients’ cash-on-hand, expenditures, and unliquidated obligations; gauges potential cost share shortfalls; cash on hand issues; and 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.

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 1 defines the key differences and similarities.

Table 1 - Enhanced Financial Monitoring Activities (Site Visit and Desk Review)

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: <ul style="list-style-type: none"> • Review grant files to verify compliance, conduct interviews to confirm adherence to approved program plans, and confirm equipment acquisition, 	The goals of FEMA’s financial site visit monitoring activities are, as applicable, to: <ul style="list-style-type: none"> • Review grant files to verify compliance, conduct interviews to confirm adherence to approved program plans, and confirm equipment acquisition, allowable use, and inventory controls;

Attribute	Desk Review	Site Visit
	<p>allowable use, and inventory controls;</p> <ul style="list-style-type: none"> • 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; • Identify and analyze relevant problems that might prevent the program from achieving its internal and external objectives; and • Provide technical assistance. 	<ul style="list-style-type: none"> • 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; • Identify and analyze relevant problems that might prevent the program from achieving its internal and external objectives; and • Provide technical assistance.

Programmatic Monitoring Overview and Approach

Programmatic monitoring involves oversight throughout the award lifecycle in order 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 National Preparedness 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.

Those programs included in the programmatic monitoring approach are listed below, including the programs subject to section 2022 of the HSA and three additional programs (THSGP, IPR, and IBSGP).

Figure 2 - Preparedness Grants Subject to Programmatic Monitoring

- | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Emergency Management Performance Grant (EMPG) • Homeland Security Grant Program (HSGP) (includes Operation Stonegarden, SHSP, and UASI) • Tribal Homeland Security Grant Program (THSGP) • Nonprofit Security Grant Program (NSGP) • Port Security Grant Program (PSGP) • Transit Security Grant Program (TSGP) • Intercity Bus Security Grant Program (IBSGP) • Intercity Passenger Rail (IPR) |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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 technical assistance 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.

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 (<https://www.fema.gov/grant-case-studies>). By accepting the award the recipient agrees to participate in a case study or evaluation if requested.

Conflicts of Interest in the Administration of Federal Awards or Subawards

To avoid conflicts of interest under grant-funded procurements and contracts, refer to the section on Procurement Integrity in the applicable NOFO, this Manual, and 2 C.F.R. §§ 200.317 – 200.326. 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 Program Analyst 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 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 his or her immediate family, or his or her partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, subapplicant, recipient, subrecipient, or FEMA employee.

Period of Performance (POP) 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 Program Analyst and must contain specific and compelling justifications as to why an extension is required. Recipients are advised to coordinate with the FEMA Program Analyst 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(is);
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 non-federal;
7. Budget outlining how remaining federal and 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 investment justification 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 grant recipient with vendors or subrecipients 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 90 days prior to the end of the POP to allow sufficient processing time. Extensions are typically granted for no more than a six-month period.

Procurement Integrity

Through audits conducted by the DHS Office of Inspector General (OIG) and FEMA grant monitoring, findings have shown that some FEMA recipients have not fully adhered to proper procurement requirements when spending grant funds. Anything less than full compliance with federal procurement requirements jeopardizes the integrity of the grant as well as the grant program.

The below highlights the Federal procurement requirements for FEMA recipients when procuring goods and services with federal grant funds. DHS will include a review of recipients' procurement practices as part of the normal monitoring activities. **All procurement activity must be conducted in accordance with Federal Procurement Standards at 2 C.F.R. §§ 200.317 – 200.326.** Select requirements under

these standards are listed below. The recipient and any of its subrecipients must comply with all requirements, even if they are not listed below.

Under 2 C.F.R. § 200.317, when procuring property and services under a federal award, states must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states must follow 2 C.F.R. § 200.322 regarding procurement of recovered materials, and 2 C.F.R. § 200.326 regarding required contract provisions.

All other non-federal entities, including tribal governments, must use their own documented procurement procedures that reflect applicable SLTT laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200. These standards include, but are not limited to, providing for full and open competition consistent with the standards of 2 C.F.R. § 200.319.

Competition and Conflicts of Interest

Among the requirements of 2 C.F.R. § 200.319(a) applicable to all non-federal entities other than states, in order to ensure objective contractor performance and eliminate unfair competitive advantage, 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 non-federal entity 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 non-federal entity.

Under this prohibition, unless the non-federal entity 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 – 200.326, 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.

Additionally, some of the situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms in order 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;
- Organizational conflicts of interest;
- 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.

Per 2 C.F.R. § 200.319(b), non-federal entities other than states must conduct procurements in a manner that prohibits the use of statutorily or administratively imposed SLTT geographical preferences in the evaluation of bids or proposals, except in those cases where applicable federal statutes expressly mandate or encourage geographic preference. Nothing in this section preempts state licensing laws. When contracting for architectural and engineering services, geographic location may be a selection criterion provided its application leaves an appropriate number of qualified firms, given the nature and size of the

project, to compete for the contract. Under 2 C.F.R. § 200.318(c)(1), non-federal entities other than states 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 which 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 non-federal entity may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, non-federal entities may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents of the non-federal entity. If the recipient or subrecipient (other than states) has a parent, affiliate, or subsidiary organization that is not a state, local government, territory, or Indian tribe, the non-federal entity must also maintain written standards of conduct covering organizational conflicts of interest. In this context, organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the non-federal entity is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization. The non-federal entity must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

Supply Schedules and Purchasing Programs

Generally, a non-federal entity may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

General Services Administration Schedules

States, tribes, and local governments, and any instrumentality thereof (such as local education agencies or institutions of higher education) may procure goods and services from a General Services Administration (GSA) schedule. GSA offers multiple efficient and effective procurement programs for state, tribal, and local governments, and instrumentalities thereof, to purchase products and services directly from pre-vetted contractors. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term government-wide contracts with commercial firms that provide access to millions of commercial products and services at volume discount pricing.

Information about GSA programs for states, tribes, and local governments, and instrumentalities thereof, can be found at <https://www.gsa.gov/resources-for/programs-for-State-and-local-governments> and <https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments>.

For tribes, local governments, and their instrumentalities that purchase off of a GSA schedule, this will satisfy the federal requirements for full and open competition provided that the recipient follows the GSA ordering procedures; however, tribes, local governments, and their instrumentalities will still need to follow the other rules under 2 C.F.R. §§ 200.317 – 200.326, such as contract cost and price (§ 200.323) and solicitation of minority, women-owned, or small businesses (§ 200.321).

Other Supply Schedules and Programs

For non-federal entities other than states, such as tribes, that want to procure goods or services from a state supply schedule, cooperative purchasing program, or other similar program, in order for such procurements to be permissible under federal requirements, the following must be true:

- The procurement of the original contract or purchasing schedule and its use by the non-federal entity complies with state and local law, regulations, and written procurement procedures;
- The state or other entity that originally procured the original contract or purchasing schedule entered into the contract or schedule with the express purpose of making it available to the non-federal entity and other similar types of entities;
- The contract or purchasing schedule specifically allows for such use, and the work to be performed for the non-federal entity falls within the scope of work under the contract as to type, amount, and geography;
- The procurement of the original contract or purchasing schedule complied with all of the procurement standards applicable to a non-federal entity other than states under at 2 C.F.R. §§ 200.317 – 200.326; and
- With respect to the use of a purchasing schedule, the non-federal entity must follow ordering procedures that adhere to applicable state, tribal, and local laws and regulations and the minimum requirements of full and open competition under 2 C.F.R. Part 200.

If a non-federal entity other than a state seeks to use a state supply schedule, cooperative purchasing program, or other similar type of arrangement, FEMA recommends the recipient discuss the procurement plans with its FEMA Program Analyst.

Procurement Documentation

Per 2 C.F.R. § 200.318(i), non-federal entities other than states and territories are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, contract type, contractor selection or rejection, and the basis for the contract price. States and territories are encouraged to maintain this information as well and 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.

Record Retention

Record Retention Period

The record retention period **may be longer than three years** in certain cases. These include:

- Records for real property and equipment acquired with Federal funds must be retained for 3 years after final disposition of the property. *See* 2 C.F.R. § 200.333(c).

- If any litigation, claim, or audit is started before the expiration of the 3-year period, the records must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken. *See* 2 C.F.R. § 200.333(a).
- The record retention period will be extended if the recipient is notified in writing of the extension by DHS/FEMA, the cognizant or oversight agency for audit, or the cognizant agency for indirect costs. *See* 2 C.F.R. § 200.333(b).
- Where DHS/FEMA requires recipients to report program income after the period of performance ends, the program income record retention period begins at the end of the recipient's fiscal year in which program income is earned. *See* 2 C.F.R. § 200.333(e).
- For indirect cost rate proposals, cost allocation plans, or other rate computation records, the start of the record retention period depends on whether the indirect cost rate documents were submitted for negotiation. If the indirect cost rate documents were submitted for negotiation, the record retention period begins from the date those documents were submitted for negotiation. If indirect cost rate documents were not submitted for negotiation, the record retention period begins at the end of the recipient's fiscal year or other accounting period covered by that indirect cost rate. *See* 2 C.F.R. § 200.333(f).

Types of Records to Retain

FEMA requires that non-federal entities maintain the following documentation for federally funded purchases:

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

Non-federal entities should keep detailed records of all transactions involving the grant. FEMA may at any time request copies of any relevant documentation and records, including purchasing documentation along with copies of cancelled checks for verification. *See, e.g.,* 2 C.F.R. §§ 200.318(i), 200.333, 200.336. In order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g). Non-federal entities who fail to fully document all purchases may find their expenditures questioned and subsequently disallowed.

Actions to Address Noncompliance

Non-federal entities receiving financial assistance 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, policies, and this Manual. 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. This potential or actual noncompliance may be discovered through routine monitoring, audits, closeout, or reporting from various sources.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R. §§ 200.207 and 200.338, FEMA may place a hold on funds until the matter is corrected, or additional information is provided per 2 C.F.R. § 200.338, or it may do both. In the event the noncompliance is not able to be corrected by imposing additional conditions or if the recipient or

subrecipient refuses to correct the matter, FEMA may use other remedies allowed under 2 C.F.R. § 200.338. These remedies include actions to disallow costs, recover funds, wholly or partly suspend or terminate the award, initiate suspension and debarment proceedings, withhold further federal awards, or take other actions that may be legally available.

FEMA may discover and take action on noncompliance even after an award has been closed. The closeout of an award does not affect FEMA's right to disallow costs and recover funds as long as the action to disallow costs takes place during the record retention period. *See* 2 C.F.R. §§ 200.333, 200.344(a). Closeout also does not affect the obligation of the non-federal entity to return any funds due as a result of later refunds, corrections, or other transactions. 2 C.F.R. § 200.344(a)(2). The types of funds FEMA might attempt to recover include, but are not limited to, improper payments, cost share reimbursements, program income, interest earned on advance payments, or equipment disposition amounts.

FEMA may seek to recover disallowed costs through a Notice of Potential Debt Letter, Remedy Notification, or other letter. The document will describe the potential amount owed, the reason why FEMA is recovering the funds, the recipient's appeal rights, how the amount can be paid, and the consequences for not appealing or paying the amount by the deadline. If the recipient neither appeals nor pays the amount by the deadline, the amount owed will become final. Potential consequences if the debt is not paid in full or otherwise resolved by the deadline include the assessment of interest, administrative fees, and penalty charges; administratively offsetting the debt against other payable federal funds; and transferring the debt to the U.S. Department of the Treasury for collection.

FEMA notes the following common areas of noncompliance for the preparedness grant programs:

- Insufficient documentation and lack of record retention.
- Failure to follow the procurement under grants requirements.
- Failure to submit closeout documents in a timely manner.
- Failure to follow EHP requirements.
- Failure to comply with the POP deadline.

Audits

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS 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. Recipients and subrecipients must retain award documents for at least three years from the date the final FFR is submitted, and longer in some cases, subject to the requirements of 2 C.F.R. § 200.333. In the case of administrative closeout, documents must be retained for at least three years from the date of closeout, or longer, subject to 2 C.F.R. § 200.333. If documents are retained longer than the required retention period, the DHS OIG, GAO, and pass-through entity, as well as FEMA in its oversight capacity, have the right to access these records as well. *See* 2 C.F.R. §§ 200.333, 200.336.

Additionally, non-federal entities must comply with the single audit requirements at 2 C.F.R. Part 200, Subpart F. Specifically, non-federal entities, other than for-profit subrecipients, that expend \$750,000 or more in federal awards during their fiscal year must have a single or program-specific audit conducted for that year in accordance with Subpart F. 2 C.F.R. § 200.501. A single audit covers all federal funds expended during a fiscal year, not just FEMA funds. The cost of audit services may be allowable per 2 C.F.R. § 200.425, but non-federal entities must select auditors in accordance with 2 C.F.R. § 200.509,

including following the proper procurement procedures. For additional information on single audit reporting requirements, see the section in this Manual titled “Single Audit Report.”

The objectives of single audits are to:

- Determine if financial statements conform to generally accepted accounting principles (GAAP);
- Determine whether the schedule of expenditures of federal awards is presented fairly;
- Understand, assess, and test the adequacy of internal controls for compliance with major programs; and
- Determine if the entity complied with applicable laws, regulations, and contracts or grants.

For single audits, the auditee is required to prepare financial statements reflecting its financial position, a schedule of federal award expenditures, and a summary of the status of prior audit findings and questioned costs. The auditee also is required to follow up and take appropriate corrective actions on new and previously issued but not yet addressed audit findings. The auditee must prepare a corrective action plan to address the new audit findings. 2 C.F.R. §§ 200.508, 200.510, 200.511.

Non-federal entities must have an audit conducted, either single or program-specific, of their financial statements and federal expenditures annually or biennially pursuant to 2 C.F.R. § 200.504. Non-federal entities must also follow the information submission requirements of 2 C.F.R. § 200.512, including submitting the audit information to the [Federal Audit Clearinghouse](#) within the earlier of 30 calendar days after receipt of the auditor’s report(s) or nine months after the end of the audit period. The audit information to be submitted include the data collection form described at 2 C.F.R. § 200.512(c) and Appendix X to 2 C.F.R. Part 200 as well as the reporting package described at 2 C.F.R. § 200.512(b).

The non-federal entity must retain one copy of the data collection form and one copy of the reporting package for three years from the date of submission to the Federal Audit Clearinghouse. 2 C.F.R. § 200.512; *see also* 2 C.F.R. § 200.517 (setting requirements for retention of documents by the auditor and access to audit records in the auditor’s possession).

FEMA, the DHS OIG, the GAO, and the pass-through entity, if applicable, as part of monitoring or as part of an audit, may review a non-federal entity’s compliance with the single audit requirements. In cases of continued inability or unwillingness to have an audit conducted in compliance with 2 C.F.R. Part 200, Subpart F, FEMA and the pass-through entity, if applicable, are required to take appropriate remedial action under 2 C.F.R. § 200.338 for noncompliance, pursuant to 2 C.F.R. § 200.505.

Disability and Limited English Proficiency Integration

Preparedness grant recipients should engage with the whole community to advance individual and community preparedness and to work as a nation to build and sustain resilience. In doing so, recipients are encouraged to consider the needs of individuals with disabilities and limited English proficiency in the activities and projects funded by the grant.

FEMA expects that the integration of the needs of people with disabilities and limited English proficiency will occur at all levels, including planning; alerting, notification, and public outreach; training; purchasing of equipment and supplies; protective action implementation; and exercises/drills. The following are examples that demonstrate the integration of the needs of people with disabilities and limited English proficiency in carrying out FEMA awards:

- Include representatives of organizations that work with/for people with disabilities on planning committees, work groups and other bodies engaged in development and implementation of the grant programs and activities.
- Hold all activities related to the grant in locations that are accessible to persons with physical disabilities to the extent practicable.
- Acquire language translation services, including American Sign Language, that provide public information across the community and in shelters.
- Ensure shelter-specific grant funds are in alignment with FEMA’s [Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters](#).
- If making alterations to an existing building to a primary function area utilizing federal funds, complying with the most recent codes and standards and making path of travel to the primary function area accessible to the greatest extent possible.
- Implement specific procedures used by public transportation agencies that include evacuation and passenger communication plans and measures for individuals with disabilities.
- Identify, create, and deliver training to address any training gaps specifically aimed toward whole-community preparedness. Include and interact with individuals with disabilities, aligning with the designated program capability.
- Establish best practices in inclusive planning and preparedness that consider physical access, language access, and information access. Examples of effective communication access include providing auxiliary aids and services such sign language interpreters, Computer Aided Real-time Translation (CART), and materials in braille or alternate formats.

FEMA grant recipients can fund projects towards the resiliency of the whole community, including people with disabilities and limited English proficiency, such as training, outreach, and safety campaigns, provided that the project aligns with the applicable NOFO, this Manual, applicable appendix to this Manual, and the terms and conditions of the award. For specific guidelines on funding a disability or limited English proficiency inclusive project, please refer to the program-specific appendix in this Manual.

National Campaigns and Programs

Preparedness grant funding can generally be used to support the following campaigns and programs that have been developed by or in partnership with DHS or FEMA.

Whole Community Preparedness

Preparedness is a shared responsibility; it 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:

- Individuals and families, including those with access and functional needs
- Businesses
- Faith-based and community organizations
- Nonprofit groups
- Schools and academia
- Media outlets
- All levels of government, including state, local, tribal, territorial, and federal partners

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

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

Additional information on incorporating whole community preparedness may be available in the applicable program-specific appendix to this Manual.

Active Shooter Preparedness

DHS aims to enhance national preparedness through a whole-community approach by providing the necessary products, tools, and resources to help all stakeholders prepare for and respond to an active shooter incident. To that end, DHS has developed a comprehensive Active Shooter Preparedness website, which includes informational resources, available at <https://www.dhs.gov/active-shooter-preparedness>.

An additional resource, the Joint DHS and Federal Bureau of Investigation (FBI) Countering Violent Extremism (CVE) and Active Shooter Web Portal is located within the Homeland Security Information Network (HSIN). The portal provides a restricted-access forum to share Unclassified, For Official Use Only (FOUO), Sensitive but Unclassified (SBU), and Law Enforcement Sensitive (LES) information. The portal provides users and training practitioners with accurate, appropriate, and relevant CVE and Active Shooter training development resources, subject-matter expert information, and outreach initiatives. It also has forums to provide feedback, products useful to others, and allows participants to ask questions concerning CVE or the Active Shooter Program. Persons with a job-related duty, public service interest, or who support a CVE and/or Active Shooter program can request access to this Portal. Additional information can be found at: <https://www.dhs.gov/cveas-portal#>.

States and Urban Areas are encouraged to review the referenced [active shooter guidance](#), evaluate their preparedness needs, and consider applying for funding to address any needs identified in this area (please see the most current Notice of Funding Opportunity (NOFO) for allowable costs). To address training needs associated with active shooter incidents, FEMA’s Emergency Management Institute provides a free, web-based training course entitled *IS-907: Active Shooter: What You Can Do*, available at the following website: <https://training.fema.gov/is/courseoverview.aspx?code=is-907>.

Soft Targets and Crowded Places

There are continued and growing threats facing Soft Targets and Crowded Places (ST-CP) throughout the nation. ST-CPs are those locations or environments that are easily accessible to large numbers of people on a predictable or semi-predictable basis that have limited security or protective measures in place. These locations are vulnerable to attack using simple tactics and readily accessible weapons such as small arms, edged weapons, vehicles, improvised explosive devices, and unmanned aerial systems. ST-CPs can include places such as town centers, shopping malls, open-air venues, outside hard targets/venues perimeters, and other places of meeting and gathering. DHS is committed to reducing the risk of attacks against ST-CPs and the impact of attacks if they do occur. However, the protection and security of ST-CPs is a shared responsibility among whole community partners including the public, ST-CP owners and operators, security industry partners, the Federal Government, and SLTT government partners. States, territories, urban areas, and public and private sector partners are encouraged to identify security gaps and build capabilities that address security needs of ST-CPs, understanding the unique challenges related to protecting locations that are open to the public. States, territories, urban areas, and public and private sector partners are also encouraged to use resources to instill a culture of awareness, vigilance, and preparedness. For more information and additional resources, please see the DHS’s [Hometown Security Program](#).

Community Lifelines

In response to recent disasters, FEMA has introduced a new lifeline construct in order to enable the continuous operation of government functions and critical business essential to human health, safety, or economic security during and after a disaster. Decision-makers must rapidly determine the scope, complexity, and interdependent impacts of a disaster. Applying the lifelines construct allows decision-makers to:

- Prioritize, sequence, and focus response efforts towards maintaining or restoring the most critical services and infrastructure;
- Utilize a common lexicon to facilitate unity of purpose among all stakeholders;
- Promote a response that facilitates unity of purpose and better communication among the whole community (federal, state, tribal, territorial, and local governments, and private sector and non-governmental entities); and
- Clarify which components of the disaster are complex (multifaceted) or complicated (difficult), requiring cross-sector coordination.

Lifelines will be used to:

- Enhance the ability to gain, maintain, and communicate situational awareness for the whole community in responding to disasters;
- Analyze impacts to the various lifelines and develop priority focus areas for each operational period during response;

- Identify and communicate complex interdependencies to identify major limiting factors hindering stabilization; and
- Update the National Response Framework to reflect use of lifelines in response planning.

Lifelines include opportunities to:

- Enable a true unity of effort between government, non-governmental organizations, and the private sector, including infrastructure owners and operators;
- Integrate preparedness efforts, existing plans, and identify unmet needs to better anticipate response requirements; and
- Refine reporting sources and products to enhance situational awareness, best determine capability gaps, and demonstrate progress towards stabilization.

For more information on lifelines, please visit <https://www.fema.gov/media-library/assets/documents/177222>.

Strategic Framework for Countering Terrorism and Targeted Violence

Terrorist organizations remain a core priority of DHS' s counterterrorism efforts and we will continue to make substantial progress in our ability to detect, prevent, protect against, and mitigate the threats that these groups pose. DHS has developed the [DHS Strategic Framework for Countering Terrorism and Targeted Violence](#) which explains how the department will use the tools and expertise that have protected and strengthened the country from foreign terrorist organizations to address the evolving challenges of today.

Program Appendix A: Homeland Security Grant Program (HSGP)

Alignment of HSGP to the National Preparedness System

The Nation uses the National Preparedness System to build, sustain, and deliver core capabilities to achieve the National Preparedness Goal (the Goal). Recipients will use the National Preparedness System to support their efforts 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 information on the National Preparedness System is available at <http://www.fema.gov/national-preparedness-system>.

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 and territories provide annual data on their proficiency across [32 core capabilities](#) through the [THIRA](#), [SPR](#), after-action reports, and other preparedness data. This data feeds into the [National Preparedness Report](#) and forms 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 this data to prioritize, synchronize, and guide programs and activities to build and sustain capabilities. 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 provides financial support to SLTT jurisdictions to help them build, sustain, and deliver core capabilities identified in the Goal. A key focus and requirement of the HSGP is 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, including risks along the Nation's borders. 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 Emergency Management Assistance Compact (EMAC).

The HSGP supports 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;
- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident; and/or
- Recover through a focus on the timely restoration, strengthening, accessibility, 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, and do so in a manner that engages the whole community while ensuring the protection of civil rights.

Reporting on the Implementation of the National Preparedness System

Identifying and Assessing Risk and Estimating Capability Requirements

By December 31, 2020, states, territories, and high-risk urban areas are required to complete a THIRA/SPR that addresses all 32 core capabilities and is compliant with Comprehensive Preparedness Guide (CPG) 201, Third Edition. Specific guidance on the requirements for each core capability will be forthcoming in 2020, as some core capabilities have fewer reporting requirements than others. Beginning in 2020, jurisdictions will also be required to respond to a series of planning-related questions as part of the THIRA/SPR.

Jurisdictions are required to submit a THIRA every three (3) years to establish a consistent baseline for assessment. While the THIRA will be only required every three years, jurisdictions will continue to be required to submit an SPR annually. For additional guidance on the THIRA/SPR, please refer to [Comprehensive Preparedness Guide \(CPG\) 201, Third Edition](#).

Reporting

- States and territories will submit their THIRA and SPR through the Unified Reporting Tool (URT) on [Prep Toolkit](#) no later than December 31 of the applicable year (every three years for THIRA and each year for SPR).
- High-risk urban areas that receive UASI funding will submit their THIRA/SPR through the URT on [Prep Toolkit](#) no later than December 31 for the years during which they have UASI funding.
- 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.

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.

Reporting

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

- Building a capability with HSGP funding
- Sustaining a capability with HSGP funding

NIMS Implementation

Recipients receiving HSGP funding are required to implement the National Incident Management System (NIMS). 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. HSGP 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 on NIMS implementation through the URT.

Planning to Deliver Capabilities

Recipients shall develop and maintain, jurisdiction-wide, all threats and hazards Emergency Operations Plans (EOPs) consistent with [Comprehensive Preparedness Guide 101, Version 2.0 \(CPG 101 v2\)](#), [Developing and Maintaining Emergency Operations Plans \(November 2010\)](#). Recipients must update their EOPs at least once every two years.

Reporting

- Recipients report EOP compliance with CPG 101 v2 in the URT.

Validating Capabilities

All recipients will develop and maintain a progressive exercise program consistent with Homeland Security Exercise and Evaluation Program (HSEEP) guidance in support of the National Exercise Program (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.

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 Training and Exercise Plan (TEP) or an Integrated Preparedness Plan (IPP). Information related to TEPs and Training and Exercise Planning Workshops (TEPWs), as well as information about IPPs and Integrated Preparedness Planning Workshops (IPPWs), can be found on the HSEEP website at <https://www.fema.gov/HSEEP> and <https://preptoolkit.fema.gov/>.

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 at: <https://www.fema.gov/national-exercise-program>, or reach out to the National Exercise Program directly at NEP@fema.dhs.gov.

- Recipients must have a current multi-year TEP or IPP that identifies preparedness priorities and activities. The current multi-year TEP or IPP must be submitted to hseep@fema.dhs.gov before January 31 of each year.
 - Recipients are encouraged to enter their exercise information into the Preparedness Toolkit at <https://preptoolkit.fema.gov/>.
- Recipients must submit After-Action Report (AAR)/Improvement Plans (IPs) to hseep@fema.dhs.gov and indicate which fiscal year's funds were used (if applicable).
- Submission of AAR/IPs must take place no later than December 31 of each year. Recipients are encouraged to submit AAR/IPs within 90 days after completion of the single exercise or progressive series.

- Recipients are encouraged to submit AAR/IPs reflecting table top exercises which validate critical plans or those reflecting large-scale functional or full-scale exercises which took place at the state, territorial, tribal, or UASI level. Recipients are discouraged from submitting AAR/IPs specific to local jurisdictions which reflect drills.
- If a recipient endures a significant real-world incident during the calendar year, they can submit the AAR from that event in place of one or more of the exercises AARs depending on the size and scale of the incident. Jurisdictions submitting real world AARs should include a request to do so with the AAR submission to hseep@fema.dhs.gov.
- Recipients can access a sample AAR/IP template at: <https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning>.

Fusion Centers

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, the Department of Justice (DOJ), Department of Health and Human Services (HHS), and other federal agencies, established the National Network of Fusion Centers (National Network), which became the backbone of the national ISE. This National Network, comprised 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 (HIDTAs), and Regional Information Sharing Systems (RISS) Centers, Joint Terrorism Task Forces (JTTFs), and major city/county intelligence units, among others.

National Network participation in the Nationwide Suspicious Activity Reporting (SAR) Initiative enables fusion centers to receive and analyze suspicious activity reporting and other tips/leads from frontline public safety personnel, the private sector, and the public, and ensure the sharing of SARs with the Federal Bureau of Investigation'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 analytic, investigative, and information-sharing focused entities to combat transnational criminal organizations in support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism. Such entities include, but are not limited to JTTFs, Area Maritime Security Committees, Border Enforcement Security Task Forces, Integrated Border Enforcement Teams, HIDTAs, and RISS Centers. Applicants should describe their collaboration plan and proposed efforts in their required Fusion Center Investment Justification.

Today's threats—including terrorism, drugs, 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 analysis of key indicators from local, state, and federal partners will enable all stakeholders to identify emerging threats and develop and implement data-driven strategies to prevent, protect against, mitigate, and respond effectively.

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 (<http://www.dhs.gov/fusion-center-locations-and-contact-information>) 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 Emerging 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 emerging 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 transnational organized criminal activity, cyber threats, and natural hazards, among others that require close collaboration with DHS operational entities such as Custom and Border Protection (CBP), Immigration and Customs Enforcement (ICE), United States Secret Service (USSS), the Cybersecurity and Infrastructure Security Agency (CISA), the United States Coast Guard (USCG), and FEMA.
- **Analytic Capability:** Fusion centers must maintain a strong analytic capability at both tactical and strategic levels to address a wide array of threats or hazards that could have implications for homeland security or national security. This capability includes, but is 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, and suspicious activity reporting; as well as necessary services and technology to facilitate analytic capabilities and collaboration.
 - Conducting routine threat assessments for 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 state authorities.
 - Maintaining an ability to routinely support federal government efforts to watchlist terrorists and transnational organized crime actors.
 - Appropriately planning for, and assessing/forecasting, prioritizing, and executing against both known and emerging threat vectors, 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 PII and includes appropriate 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 aided dispatch (CAD) and record management systems (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), and license plate reader technologies.

- **Interagency Collaboration:** Fusion centers must maintain strong partnerships to enable 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 and operational 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 are listed at <http://www.dhs.gov/homeland-security-grant-program-hsgp>.
- DHS/FEMA approved analyst courses that meet the grant requirement are listed at <http://www.dhs.gov/fema-approved-intelligence-analyst-training-courses>.

Through the Program Performance Report (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, Area Maritime Security Committees, Border Enforcement Security Task Forces, Integrated Border Enforcement Teams, HIDTAs, and RISS Centers. **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 Fusion Center Assessment.**

Continuity of Operations

Continuity planning and operations are an inherent element of each core capability and the coordinating structures that provide them. Continuity operations 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 the Continuity Guidance Circular (CGC) for federal and SLTT governments, non-governmental organizations, and private sector critical infrastructure owners and operators. Federal Continuity Directives (FCDs) establish continuity program and planning requirements for executive departments and agencies. This direction and guidance assists 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.

Presidential Policy Directive 40, FCD 1, FCD 2, and CGC outline the overarching continuity requirements and guidance for organizations and provides methodology and checklists. For additional information on continuity programs, guidance, and directives, visit <https://www.fema.gov/continuity-guidance-circular-cgc> and <https://www.fema.gov/national-continuity-programs>.

Governance

In keeping with the guiding principles of governance for all FEMA preparedness programs, recipients must coordinate activities across preparedness disciplines and levels of government, including state, territorial, local, and tribal 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. Specific attention should be paid to how available preparedness funding sources can effectively support a whole community approach to emergency preparedness and management and the enhancement of core capabilities. To ensure this, the SAA must establish or reestablish a unified Senior Advisory Committee (SAC). Additionally, urban areas are required to establish Urban Area Working Groups (UAWGs) representative of the counties, cities, towns, and tribes within the high-risk urban area, including, as appropriate, representatives of rural jurisdictions, high-population jurisdictions, and high-threat jurisdictions.

Senior Advisory Committee (SAC)

The SAC builds upon previously established advisory bodies under the SHSP, UASI program, Nonprofit Security Grant Program (NSGP), Transit Security Grant Program (TSGP), and Port Security Grant Program (PSGP). Examples of advisory bodies that should be included on a SAC include UAWGs, Statewide Interoperability Governing Boards (SIGB), Area Maritime Security Committees (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.

SAC Composition and Scope

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

- Individuals from the counties, cities, towns, and Indian tribes within the state or high-risk urban area, including, as appropriate, representatives of rural, high-population, and high-threat jurisdictions of UASI-funded 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)
- Statewide Interoperability Coordinator (SWIC) and Statewide Interoperability Governing Body (SIGB) members
- Citizen Corps Whole Community Councils
- Local or tribal government officials
- Tribal organizations
- 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
- 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 (HSA) (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 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, response, and recovery activities within the State, and include representation from the stakeholder groups and disciplines identified above.

The above membership requirement does not prohibit states, 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 Point of Contacts (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 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, individuals with limited English proficiency and others with access and functional needs, socio-economic factors and cultural diversity 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 ND Grants. SAAs will use the URT to verify compliance with SAC charter requirements.

SAC 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;
- Management of all available preparedness funding sources to ensure their effective use and to minimize duplication of effort;
- Ensuring investments support closing capability gaps or sustaining capabilities identified in the THIRA/SPR;

- Assist in preparation and revision of the state, regional, or local homeland security plan or the threat and hazard identification and risk assessment, as the case may be; and
- Assist in determining effective funding priorities for SHSP grants.

SAC Charter

The governance of the SHSP and UASI programs 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 Program Analyst. 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 state's and UASI'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.

Urban Area Working Group (UAWG)

UASI program implementation and governance must include regional partners and should have balanced representation among entities with operational responsibilities for prevention, protection, mitigation, response, and recovery activities within the region. In some instances, high-risk urban area boundaries cross state borders. States must ensure that the identified urban areas take an inclusive regional approach to the development and implementation of the UASI program 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.

UAWG Composition and Scope

Pursuant to section 2003(b) of the *Homeland Security Act of 2002* (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 (MSAs), as defined by the Office of Management and Budget (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 at <https://www.census.gov/programs-surveys/metro-micro.html>.

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 Whole Community Citizen Corps Council and tribal representatives. The UAWG should also include at least one representative from each of the following significant stakeholders:

- Local or 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
- State and regional interoperable communications coordinators, as appropriate state and major urban area fusion centers, as appropriate

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

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 ND Grants. High-risk urban areas must notify the SAA and the FEMA Headquarters Program Analyst of any updates to the UAWG structure or membership after the application is submitted.

UAWG Responsibilities

UAWGs must ensure that applications for funding under the UASI program support 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 program. 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.

UAWG 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 management and administration responsibilities, and funding allocation methodologies are formalized in a working group charter or another form of standard operating procedure related to the UASI program 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 ND Grants 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 program.

Supplemental SHSP and UASI Guidance

Collaboration

Collaboration with Other Federal Preparedness Programs

FEMA strongly encourages states, high-risk urban areas, tribes, 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 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 Law Enforcement Support Office (LESO) Program); and the Resilience Directorate/Office of Infrastructure Protection’s (OIP) Regional Resilience Assessment Program (RRAP). However, coordination is not limited to grant funding. It also includes leveraging assessments such a Transportation Security Agency’s (TSA) Baseline Assessment and Security Enhancement (BASE), reporting from the Intelligence Community, risk information such as U.S. Coast Guard’s Maritime Security Risk Analysis Model (MSRAM), and United States Border Patrol (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 the U.S. Department of Transportation’s (DOT) National Highway Traffic Safety Administration (NHTSA). Other federal agencies participating in the Emergency Preparedness Grant Coordination process are working to identify current preparedness activities and areas for collaboration across federal

grants with public health and healthcare preparedness components. The participating other federal agencies include:

- HHS ASPR
- HHS CDC
- HHS Health Resources and Services Administration (HRSA)
- DOT NHTSA

Federal agencies are actively coordinating guidance and technical assistance and encourage all recipients to actively coordinate preparedness activities for their jurisdictions. More information on the Emergency Preparedness Grant Coordination process can be found [here](#).

Collaboration with Health Care Coalitions (HCCs)

HCCs 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 2017-2022 Health Care Preparedness and Response Capabilities (<https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/2017-2022-healthcare-pr-capabilities.pdf>).

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.

Collaboration with Tribes

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.

Whole Community Preparedness

SHSP and UASI recipients should engage with the whole community to advance community and individual preparedness and to work as a nation to build and sustain resilience. Recipients should consider the three goals of the 2018-2022 FEMA Strategic Plan in their program design and delivery, specifically Strategic Goal 1: Build a Culture of Preparedness and Strategic Goal 2: Ready the Nation for Catastrophic Disasters. Recipients should integrate program design and delivery practices that ensure representation and services for under-represented diverse populations that may be more impacted by disasters including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity, and other underserved populations. Individual preparedness must be coordinated by an integrated body of government and nongovernmental representatives as well, including but not limited to, elected officials, the private sector (especially privately owned critical infrastructure), private nonprofits, nongovernmental organizations (including faith-based, community-based, and voluntary organizations), advocacy groups for under-represented diverse populations that may be more impacted by disasters including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity, and other underserved populations.

In addition to Community Emergency Response Team (CERT) programs, the following preparedness programs are allowable expenses:

- **Financial Preparedness Activities** that encourage and assist Americans in preparing for the true cost of disasters. Allowable activities include encouraging emergency savings, promoting home and renter’s insurance, and promoting flood insurance for individuals and families. Partnerships with local financial wellness organizations such as credit unions, financial counselors, community banks, and others that reach a variety of audiences are encouraged.
- **Preparedness of Community-Based Organizations** that serve as a critical safety net for Americans disproportionately impacted by disasters. Examples of community-based organizations include but are not limited to food banks, food pantries, homeless shelters, school readiness and after school centers, adult day care centers, job training centers, legal assistance centers, and cultural centers. Allowable activities include Whole Community exercises, trainings, and activities focused on staff preparedness, information sharing with clients and government, and continuity of essential functions in the event of an emergency.
- **Youth Preparedness Resources** to support practitioners as they create and run programs in their communities are available at www.ready.gov/kids. The interactive website is a one-stop shop with search features, tools, and resources for parents, caregivers, and educators to help engage kids and young people on emergency and disaster preparedness. Site visitors can find information, programs, curricula, and games and activities that engage and teach youth and their families to be prepared. Ready.gov/kids also has resources to support the integration and implementation of children’s disaster-related needs into preparedness, planning, response and recovery efforts initiated by state, local, territorial and tribal governments, and stakeholders responsible for the temporary care of children.

Supplemental Operation Stonegarden Grant (OPSG) Program Guidance

OPSG supports enhanced cooperation and coordination among Customs and Border Protection (CBP), United States Border Patrol (USBP), and federal, state, local, tribal, and territorial 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 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. OPSG also further enhances the sharing of threat information and intelligence between federal, state, local, tribal, and territorial 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, and suspicious activity reporting, as well as necessary services and technology to facilitate analytic capabilities and collaboration.

State, local, tribal, and territorial (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 *Immigration and Nationality Act*).

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.
- 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 and suspicious activity reporting, 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 Integrated Planning Team (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.
- No fewer than two IPT meetings must take **place during every funding year:**
 - Prior to submitting the Concept of Operations (application)
 - Prior to submitting the Campaign Plan
- OPSG funds may be used for travel and per diem in support of the IPTs and OPSG strategic planning events as long as the costs are otherwise compliant with other program and regulatory requirements.

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
- 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, DC, 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.

Transportation Costs and Costs Related to the Provision of Acute Medical Care

Please see [Information Bulletin No. 438](#) for information on transportation costs and costs related to the provision of acute medical care under an OPSG award.

HSGP Funding Guidelines

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 Program Analyst prior to making any investment that does not clearly meet the allowable expense criteria. Funding guidelines established within this section support the five mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and associated core capabilities within the Goal. 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 closing capability gaps or sustaining capabilities identified in the THIRA/SPR. 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.

Multiple Purpose or Dual-Use of Funds

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 *Homeland Security Act of 2002* (6 U.S.C. § 609(c)).

Planning (SHSP and UASI)

SHSP and UASI funds may be used for a range of emergency preparedness and management planning activities such as those associated with the development, review, and revision of the THIRA, SPR, continuity of operations plans, and other planning activities that support the Goal and placing an emphasis on updating and maintaining a current EOP that conforms to the guidelines outlined in [CPG 101 v2](#).

Organization (SHSP and UASI)

States and high-risk urban areas must justify proposed expenditures of SHSP or UASI funds to support organization activities within their Investment Justification (IJ) submission. Organizational activities include:

- Program management

- Development of whole community partnerships, through groups such as Citizen Corp Councils
- Structures and mechanisms for information sharing between the public and private sector
- Implementing models, programs, and workforce enhancement initiatives to address ideologically inspired radicalization to violence in the homeland
- Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors
- Operational Support
- Utilization of standardized resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident
- Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS) or needs resulting from a National Special Security Event
- Paying salaries and benefits for personnel to serve as qualified Intelligence Analysts. Per the *Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act (PRICE Act)*, Pub. L. No. 110-412, § 2, codified in relevant part, as amended, at 6 U.S.C. § 609(a), SHSP and UASI funds may be used to hire new staff and/or contractor positions to serve as intelligence analysts to enable information/intelligence sharing capabilities, as well as support existing intelligence analysts previously covered by SHSP or UASI funding. *See* 6 U.S.C. § 609(a). To be hired as an intelligence analyst, staff and/or contractor personnel must meet at least one of the following criteria:
 - Complete training to ensure baseline proficiency in intelligence analysis and production within six months of being hired; and/or,
 - Previously served as an intelligence analyst for a minimum of two years either in a federal intelligence agency, the military, or state and/or local law enforcement intelligence unit.
- All fusion center analytical personnel must demonstrate qualifications that meet or exceed competencies identified in the Common Competencies for state, local, and tribal intelligence analysts, which outlines the minimum categories of training needed for intelligence analysts. A certificate of completion of such training must be on file with the SAA and must be made available to the recipient's respective FEMA HQ Program Analyst upon request.

All SAAs are allowed to use up to 50% of their SHSP funding, and all high-risk urban areas are allowed to use up to 50% of their UASI funding, for personnel costs per 6 U.S.C. § 609(b)(2)(A). Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, intelligence analysts, and Statewide Interoperability Coordinators (SWICs).

At the request of a recipient, the FEMA Administrator (or their designee) may grant a waiver of this 50% limitation under 6 U.S.C. § 609(b)(2)(B). Requests for waivers to the personnel cap must be submitted by the authorized representative of the SAA to FEMA in writing on official letterhead, with the following information:

- Documentation explaining why the cap should be waived
- Conditions under which the request is being submitted
- A budget and method of calculation of personnel costs both in percentages of the grant award and in total dollar amount.

Please see [IB 421b](#) for additional information on the waiver request process.

Organizational activities under SHSP and UASI include:

Operational Overtime Costs. In support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism and other catastrophic events, operational overtime costs are allowable for increased protective security measures at critical infrastructure sites or other high-risk locations and to enhance public safety during mass gatherings and high-profile events. In that regard, HSGP recipients are urged to consider using grant funding to support soft target preparedness activities. SHSP or UASI funds may be used to support select operational expenses associated with increased security measures in the authorized categories cited in the table below, but this table is not exhaustive. FEMA retains the discretion to approve other types of requests that do not fit within one of the categories of the table.

Table 2 - Authorized Operational Overtime Categories

	Category	Description
1	National Terrorism Advisory System (NTAS)	Security measures in response to an increase in the threat level under the NTAS to an “elevated” or “imminent” alert status. FEMA Information Bulletin No. 367, Impact of National Terrorism Advisory System on Homeland Security Grant Programs , remains applicable; therefore, advance authorization from FEMA is not required. Refer to https://www.dhs.gov/topic/ntas for additional information on the NTAS.
2	National Security Special Event (NSSE)	Security measures for a designated NSSE. NSSEs are events of national or international significance deemed by DHS to be a potential target for terrorism or other criminal activity.
3	Special Event Assessment Rating (SEAR) Level 1 through Level 4 Events	<p>Security measures required for SEAR Level 1 through Level 4 events as designated by DHS and included in the DHS National Special Events List, as defined below:</p> <ul style="list-style-type: none"> • SEAR 1: A significant event with national and/or international importance that may require extensive federal interagency support; • SEAR 2: A significant event with national and/or international importance that may require some level of federal interagency support. • SEAR 3: An event of national and/or international importance that requires only limited federal support. • SEAR 4: An event with limited national importance that is managed at state and local level. <p>NOTE: In cases where a threat of terrorism can be associated with a SEAR Level 5 event, the event planners should coordinate with their state or territory Homeland Security Advisor to seek re-adjudication of the SEAR rating. Operational overtime for security measures associated with such events will be considered for approval by FEMA if re-adjudication results in a SEAR 1 through 4 rating.</p>
4	States of Emergency	Declarations of states of emergency by the Governor associated with a terrorism-related threat or incident. This excludes Presidentially declared major disasters or emergencies where federal funding support for the proposed grant-funded activity is made available

	Category	Description
		through the FEMA Public Assistance program or other federal disaster grants.
5	National Critical Infrastructure Prioritization Program (NCIPP)	Protection of Level 1 and Level 2 facilities identified through DHS's NCIPP based on a terrorism-related threat to critical infrastructure.
6	Directed Transit Patrols	Targeted security patrols in airports and major transit hubs based on a terrorism-related threat to transportation systems.
7	Other Related Personnel Overtime Costs	Overtime costs may be authorized for personnel assigned to directly support any of the security activities relating to the categories above. Examples include firefighters and emergency medical services personnel; public works employees who may be responsible for installing protective barriers and fencing; public safety personnel assigned to assist with event access and crowd control; emergency communications specialists; fusion center analysts; National Guard; contract security services; etc.
8	Operational Support to a Federal Agency	Overtime costs are allowable for personnel to participate in information, investigative, and intelligence sharing activities related to homeland security/terrorism preparedness and specifically requested by a federal agency. Allowable costs are limited to overtime associated with federally requested participation in eligible activities, including anti-terrorism task forces, JTTFs, Area Maritime Security Committees (as required by the <i>Maritime Transportation Security Act of 2002</i>), DHS Border Enforcement Security Task Forces, and Integrated Border Enforcement Teams. In addition, reimbursement for operational overtime law enforcement activities related to combating transnational crime organizations in support of efforts to enhance capabilities for detecting, deterring, disrupting, and preventing acts of terrorism is an allowable expense under SHSP and UASI on a case-by-case basis. Grant funding can only be used in proportion to the federal man-hour estimate and only after funding for these activities from other federal sources (i.e., FBI JTTF payments to state and local agencies) has been exhausted.

All allowable operational overtime costs are also subject to the administration requirements outlined in the following subsection.

Administration of Operational Overtime Requests

- Except for an elevated NTAS alert, SHSP or UASI funds may only be spent for operational overtime costs upon prior written approval by FEMA. The SAA must submit operational overtime requests in writing to its assigned FEMA Program Analyst (PA). FEMA will consider requests for special event activities up to one year in advance. However such requests must be within the award's current POP and must not result in the need for a request to extend the period of performance. SAAs should contact the Centralized Scheduling and Information Desk (CSID)

for PA contact information. CSID can be reached by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

- All operational overtime requests must clearly explain how the request meets the criteria of one or more of the categories listed in the table above. Requests must address the threat environment as it relates to the event or activity requiring operational overtime support and explain how the overtime activity is responsive to the threat. Request letters sent to FEMA must be UNCLASSIFIED but may be labeled “For Official Use Only.” If explaining the threat will require the sharing of classified information, the letter should state that fact. FEMA will then plan for the sharing of classified information through official channels.
- Post-event operational overtime requests will only be considered on a case-by-case basis, where it is demonstrated that exigent circumstances prevented submission of a request in advance of the event or activity.
- Under no circumstances may DHS/FEMA grant funding be used to pay for costs already supported by funding from another federal source.
- States with UASI jurisdictions can use funds retained at the state level to reimburse eligible operational overtime expenses incurred by the state (per the above guidance limitations). 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 DHS/FEMA upon request demonstrating how any UASI funds retained by a state would directly support the high-risk urban area.
- FEMA will consult and coordinate with appropriate DHS components as necessary to verify information used to support operational overtime requests. For example, the review of operational overtime requests for the protection of critical infrastructure will be coordinated with DHS Office of Cyber and Infrastructure Analysis to verify the Level I or Level II NCIPP designation. Also, DHS Office of Intelligence and Analysis will be consulted to validate reported threat information associated with the event or activity.

Personnel Costs. Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable HSGP planning, training, exercise, and equipment activities. Personnel may include but are not limited to training and exercise coordinators, program managers for activities directly associated with SHSP and UASI funded activities, intelligence analysts, and Statewide interoperability coordinators (SWIC).

For further details, SAAs should refer to [Information Bulletin No. 421b](#), Clarification on the Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act of 2008 (Public Law 110-412 – the PRICE Act), October 30, 2019, or contact their FEMA PA. HSGP funds may not be used to support the hiring of any personnel to fulfil traditional public health and safety duties nor to supplant traditional public health and safety positions and responsibilities. The following definitions apply to personnel costs:

- *Hiring.* State and local entities may use grant funding to cover the salary of newly hired personnel who are exclusively undertaking allowable DHS/FEMA grant activities as specified in this guidance. This may not include new personnel who are hired to fulfill any non-DHS/FEMA program activities under any circumstances. Hiring will always result in a net increase of Full Time Equivalent (FTE) employees.
- *Overtime.* These expenses are limited to the additional costs that result from personnel working over and above 40 hours of weekly work time as the direct result of their performance of DHS/FEMA-approved activities specified in this guidance. Overtime associated with any other activity is not eligible.
- *Backfill-Related Overtime.* Also called “Overtime as Backfill,” these expenses are limited to overtime costs that result from personnel who are working overtime (as identified above) to

perform the duties of other personnel who are temporarily assigned to DHS/FEMA-approved activities outside their core responsibilities. Neither overtime nor backfill expenses are the result of an increase of FTE employees.

- *Supplanting*. Grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated 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.

OPSG funds may be used for domestic travel and *per diem*, including costs associated with the deployment/redeployment of personnel to border areas and for travel associated with law enforcement entities assisting other local jurisdictions in law enforcement activities. In addition, allowable costs include supporting up to six-month deployment of law enforcement personnel to critical Southwest Border locations for operational activities (travel costs must be in accordance with applicable travel regulations).

Organization (OPSG)

Operational Overtime Costs

OPSG funds should be used for operational overtime costs associated with law enforcement activities in support of border law enforcement agencies for increased border security enhancement. Overtime pay is for enhanced patrol for certified public safety officers, along with limited support for other law enforcement direct support personnel (e.g., Communication Officers/Dispatchers, non-sworn patrol pilots, etc.). Overtime shall be reimbursed consistent with the non-federal entity's overtime policy and the requirements as stated below:

- Overtime is time worked that exceeds the required number of hours during an employee's designated shift.
- Overtime must be worked to increase patrol capacity and be in support of identified and approved USBP border security operations.
- The OPSG overtime hourly rate of pay will be no more than the approved overtime rate per local law and policy and must be in accordance with applicable state and federal regulations.
- All overtime expenses under OPSG must be reasonable for the services rendered and conform to the non-federal entity's established written policy, which must apply to both federally funded and non-federally funded activities and comply with the other applicable requirements under 2 C.F.R. §§ 200.430-200.431.
- The non-federal entity may not utilize OPSG funding to pay for an employee's overtime hours or pay that exceeds 16 hours worked in any 24-hour period.

Personnel Costs

Up to 50% of an OPSG award may be used to pay for all personnel costs (only to the extent that such expenses are for the allowable activities within the scope of the grant). At the request of a recipient or subrecipient, the FEMA Administrator (or designee) may waive the 50% personnel cap. Waiver decisions are at the discretion of the FEMA Administrator and will be considered on a case-by-case basis in accordance with [IB 421b](#). 6 U.S.C. § 609(b)(2). A formal OPSG personnel waiver request should:

- Be on official letterhead, include a written justification, and be signed by the local jurisdiction.
- Include a budget and method of calculation of personnel costs both in the percentage of the grant award and in total dollar amount, reflecting the change in scope or objective to the project.
- Include an approved Operations Order from the USBP Sector office that supports the local jurisdiction's written justification.
- Be coordinated with the USBP Sector, SAA, and the DHS/CBP Office of the Border Patrol (OBP).

Further, changes in scope or objective also require FEMA's prior written approval pursuant to 2 C.F.R. § 200.308(c)(1)(i). If the cost changes are allowable under the grant, a Fragmentary Order (FRAGO) must be submitted to HSIN to obtain FEMA's prior written approval of such changes in accordance with 2 C.F.R. § 200.308(c)(1)(i). These modifications will be annotated in the annex section of the FRAGO.

OPSG funds may be used to pay additional current part-time law enforcement personnel salaries to bring them to temporary full-time status. OPSG funds may support a Governor's request to activate, deploy, or redeploy specialized National Guard Units/Package and/or elements of state law enforcement serving as friendly forces to increase or augment specialized/technical law enforcement elements' operational activities. Costs associated with backfill for personnel supporting operational activities are allowable.

As with all OPSG personnel costs, OPSG grant funds will be used to supplement existing funds and will not replace (supplant) funds that have been appropriated 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.

Intelligence Support

OPSG funds may as applicable and operationally beneficial be used to pay salaries and benefits for personnel to serve as qualified Intelligence Analysts. Per the 6 U.S.C. § 609(a), OPSG funds may be used to hire new staff and/or contractor positions to serve as intelligence analysts to enable and enhance information/intelligence sharing capabilities, as well as support existing intelligence analysts previously covered by OPSG funding. *See* 6 U.S.C. § 609(a). Qualified OPSG-funded intelligence analysts can be assigned to an applicable law enforcement facility/intelligence function as long as information/intelligence sharing is maintained. To serve as an OPSG-funded intelligence analyst, staff and/or contractor personnel must meet at least one of the following criteria:

- Complete training to ensure baseline proficiency in intelligence analysis and production within six months of being hired; and/or,
- Previously served as an intelligence analyst for a minimum of two years either in a federal intelligence agency, the military, or state and/or local law enforcement intelligence unit.

OPSG-funded intelligence analysts must demonstrate qualifications that meet or exceed competencies identified in the Common Competencies for state, local, and tribal intelligence analysts, which outlines the minimum categories of training needed for intelligence analysts. A certificate of completion of such training must be on file with the SAA and must be made available to the recipient's respective FEMA HQ Program Analyst upon request.

As with all allowable expenditures under HSGP, the SAA or its OPSG subrecipient jurisdictions must agree to and approve the use of funds for this purpose and request to amend applicable grant awards accordingly. Under OPSG, SAAs and subrecipients requesting to use grant funds in this manner must also collaborate regarding prioritization of funds for the provision of allowable associated costs for intelligence analysts with the applicable USBP sector and memorializing the collaboration through an

Operations, Fragmentary or Supplemental Operations Order approved by the USBP sector, USBP Headquarters, and the FEMA Grant Programs Directorate.

Temporary or Term Appointments

- Subrecipients may utilize temporary or term appointments to augment the law enforcement presence on the borders. However, applying funds toward hiring full-time or permanent sworn public safety officers is unallowable.
- OPSG-funded temporary or term appointments may not exceed the approved period of performance.
 - For OPSG purposes, temporary appointments are non-status appointments for less than one year.
 - For OPSG purposes, term appointments are non-status appointments for one year, extendable for one year as necessary.
- OPSG funding for temporary or term appointments may pay for salary only. Benefits are not allowable expenses for term or temporary employees.
- OPSG remains a non-hiring program. Appropriate uses of temporary or term appointments include:
 - To carry out specific enforcement operations work for ongoing OPSG-funded patrols throughout the Sector Area of Operation;
 - To staff operations of limited duration; such as OPSG-enhanced enforcement patrols targeting specific locations or criminal activity; and,
 - To fill OPSG positions in activities undergoing transition or personnel shortages and local backfill policies (medical/military deployments)
- OPSG term and temporary appointments must have all necessary certifications and training to enforce state and local laws. OPSG funds will not be used to train or certify term or temporary appointments except as otherwise stated in the OPSG section of this manual and the HSGP NOFO.
- DHS/FEMA provides no guarantee of funding for temporary or term appointments. In addition to the terms of this manual and the HSGP NOFO, subrecipients must follow their own applicable policies and procedures regarding temporary or term appointments.

Management and Administration (M&A) (OPSG)

Management and administration (M&A) activities are those directly relating to the management and administration of OPSG funds, such as financial management and monitoring. Recipients may retain up to 2.5% of the overall OPSG allocation prior to passing-through funding to subrecipients. This funding must be deducted in an equal percentage from each subrecipient. Subrecipients and friendly forces may retain funding for M&A purposes; however, the total amount retained cannot exceed 5% of the subrecipient's subaward. Friendly forces are local law enforcement entities that are subordinate subrecipients under OPSG. In other words, friendly forces are entities that receive a subaward from a subrecipient under the OPSG program. Friendly forces must comply with all requirements of subrecipients under 2 C.F.R. Part 200.

Equipment (SHSP and UASI)

The 21 allowable prevention, protection, mitigation, response, and recovery equipment categories for HSGP are listed on the Authorized Equipment List (AEL). The AEL is available at <http://www.fema.gov/authorized-equipment-list>. Some equipment items require prior approval from DHS/FEMA before obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required or to ensure prior approval is obtained if necessary.

Unless otherwise stated, all equipment must meet all mandatory regulatory and/or DHS/FEMA-adopted standards to be eligible for purchase using these funds. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable [SAFECOM Guidance](#). Such investments must be coordinated with the SWIC and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

Grant funds may be used for the procurement of medical countermeasures. Procurement of medical countermeasures must be conducted in collaboration with state, city, or local health departments that administer federal funds from HHS for this purpose and with existing MMRS committees where available, to sustain their long-term planning for appropriate, rapid, and local medical countermeasures, including antibiotics and antidotes for nerve agents, cyanide, and other toxins. Procurement must have a sound threat-based justification with an aim to reduce the consequences of mass casualty incidents during the first crucial hours of a response. Prior to procuring pharmaceuticals, recipients must have in place an inventory management plan to avoid large periodic variations in supplies due to coinciding purchase and expiration dates. Recipients are encouraged to enter into rotational procurement agreements with vendors and distributors. Purchases of pharmaceuticals must include a budget for the disposal of expired drugs within each fiscal year's POP for HSGP. The cost of disposal cannot be carried over to another DHS/FEMA grant or grant period.

EMS electronic patient care data systems should comply with the most current data standard of the National Emergency Medical Services Information System (www.NEMSIS.org).

Equipment (OPSG)

OPSG equipment is intended to be incidental to the enhanced border security operations being performed. The grant is not intended to be used to outfit or supply general equipment to SLTT law enforcement agencies. Equipment must be relatable to and justified by the operational benefit it will provide. Each appropriate OPSG sector coordinator is required to keep an inventory of OPSG purchased equipment that includes at a minimum: 1) grant funding year; 2) purchase amount; 3) purchase date; 4) purchase quantity; 5) equipment ID; 6) source of funding for the property, including the Federal Award Identification Number; 7) who holds title to the property; 8) federal share percent of the property; 9) location of the property; 10) use and condition of the property; 11) disposal date; and 12) brief disposal justification information and sale price if sold. Each Operations Order/FRAGO will require that each friendly force submit the equipment inventory for each Operations Order/FRAGO submission.

- **Equipment Marking.** Because equipment purchased with OPSG funding is intended to be used to support OPSG activities, it **may** be appropriately marked to ensure its ready identification and primary use for that purpose. **When practicable**, any equipment purchased with OPSG funding **should** be prominently marked as follows: "**Purchased with DHS funds for Operation Stonegarden Use**".
- **Fuel Cost and Mileage Reimbursement.** There is no cap for reimbursement of fuel or mileage costs in support of operational activities. Subrecipients and friendly forces may not claim reimbursements for both mileage and fuel/maintenance for the same equipment at the same time.
- **Vehicle and Equipment Acquisition, Including Leasing and Rentals.** Allowable purchases under OPSG include patrol vehicles and other mission-specific equipment whose primary purpose is to increase operational capabilities on or near a border nexus in support of approved border security operations. A detailed justification must be submitted to the respective FEMA HQ Program Analyst prior to purchase.
- **Medical Emergency Countermeasures:** Allowable purchases under OPSG include narcotic

antagonist pharmaceuticals, detection and identification equipment, safe storage and transportation, personnel protective equipment, and initial equipment training, as reflected in the AEL and explained in [IB 438](#).

Requirements for Small Unmanned Aircraft System (SHSP, UASI, and OPSG)

All requests to purchase Small Unmanned Aircraft Systems (SUAS) with FEMA grant funding must comply with [IB 426](#) and [IB 438](#) and also include a description of the policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties of the jurisdiction that will purchase, take title to or otherwise use the SUAS equipment.

Training (SHSP and UASI)

Allowable training-related costs under HSGP include the establishment, support, conduct, and attendance of training specifically identified under the SHSP and UASI program and/or in conjunction with emergency preparedness training by other federal agencies (e.g., HHS and DOT). Training conducted using HSGP funds should address a performance gap identified through a TEP or other assessments (e.g., National Emergency Communications Plan NECP Goal Assessments) and contribute to building a capability that will be evaluated through a formal exercise. Any training or training gaps, including training related to under-represented diverse populations that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations, should be identified in a TEP and addressed in the state or high-risk urban area training cycle. Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model of instructional design.

Recipients are also encouraged to utilize the National Training and Education Division's National Preparedness Course Catalog. Trainings include programs or courses developed for and delivered by institutions and organizations funded by DHS/FEMA/National Training and Education Division (NTED). This includes the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and NTED's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (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, state, local, territorial, and tribal audiences. All courses have been approved through NTED's course review and approval process. The catalog can be accessed at <http://www.firstrespondertraining.gov>.

Exercises (SHSP and UASI)

Exercises conducted with grant funding should be managed and conducted consistent with HSEEP. HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at <https://www.fema.gov/exercise>.

Maintenance and Sustainment (SHSP, UASI, and OPSG)

The use of DHS/FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, as described in FEMA Policy [FP 205-402-125-1](#) under all active and future grant awards, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the POP of the specific grant funds used to purchase the plan or warranty.

Grant funds are intended to support the Goal by funding projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in FEMA's [IB 379, Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#), initially for FY 2007-2011, allows for the expansion of eligible maintenance and sustainment costs which must be in (1) direct support of existing capabilities; (2) must be an otherwise allowable expenditure under the applicable grant program; (3) be tied to one of the core capabilities in the five mission areas contained within the Goal, and (4) shareable through the Emergency Management Assistance Compact. Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant or any other source of funding other than DHS/FEMA preparedness grant program dollars.

Law Enforcement Terrorism Prevention Activities Allowable Costs (SHSP and UASI)

Activities eligible for the use of Law Enforcement Terrorism Prevention Activities (LETPA) focused funds include but are not limited to:

- Maturation and enhancement of designated state and major high-risk urban area fusion centers, including information sharing and analysis, threat recognition, terrorist interdiction, and training/ hiring of intelligence analysts;
- Coordination between fusion centers and other analytical and investigative efforts including, but not limited to JTTFs, Field Intelligence Groups (FIGs), HIDTAs, RISS Centers, criminal intelligence units, and real-time crime analysis centers;
- Implementation and maintenance of the nationwide SAR Initiative, including training for front-line personnel on identifying and reporting suspicious activities;
- Implementation of the “If You See Something, Say Something®” campaign to raise public awareness of indicators of terrorism and terrorism-related crime and associated efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS “If You See Something, Say Something®” campaign using grant funds work directly with the DHS Office of Partnership and Engagement (OPE) to ensure all public awareness materials (e.g., videos, posters, tri-folds, etc.) are consistent with the DHS’s messaging and strategy for the campaign and compliant with the initiative’s trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the Campaign’s Office (seesay@hq.dhs.gov), must be facilitated by the FEMA HQ Program Analyst;
- Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical infrastructure site or at-risk nonprofit organizations; and
- Building and sustaining preventive radiological and nuclear detection capabilities, including those developed through the Securing the Cities initiative.
- Integration and interoperability of systems and data, such as CAD and RMS, to facilitate the collection, evaluation, and assessment of suspicious activity reports, tips/leads, and online/social media-based threats.

Law Enforcement Readiness (SHSP, UASI, and OPSG)

OPSG grant funds may be used to increase operational, material, and technological readiness of SLTT law enforcement agencies. The Delegation of Immigration Authority, Section 287(g) of the *Immigration and Nationality Act (INA)* program allows a state or local law enforcement entity to enter into a

partnership with ICE, under a joint Memorandum of Agreement (MOA), to receive delegated authority for immigration enforcement within their jurisdictions. SHSP, UASI, or OPSG grant funds may be requested and may be approved on a case-by-case basis for immigration enforcement training in support of the border security mission. Requests for training will be evaluated on a case-by-case basis and can only be used for certification in the section 287(g) program provided by DHS/ICE. SHSP, UASI, or OPSG subrecipients with agreements under section 287(g) of the *INA* (8 U.S.C. § 1357(g)) to receive delegated authority for immigration enforcement within their jurisdictions may also be reimbursed for section 287(g) related operational activities with approval from FEMA on a case-by-case basis. For OPSG, subrecipients must be authorized by USBP Headquarters and Sectors, and operational activities must be coordinated through a USBP Sector.

Regional Border Projects (OPSG)

Recipients are encouraged to prioritize the acquisition and development of regional projects on the borders to maximize interoperability and coordination capabilities among federal agencies and with state, local, and tribal law enforcement partners. Such regional projects include:

- Communications equipment:
- Radio systems and repeaters
- Integration with regional intelligence and information sharing effort (i.e. fusion centers)
 - Intelligence analysts
- Situational Awareness equipment:
 - License Plate Reader Networks
 - Visual detection and surveillance systems
 - Sensor Systems
 - Radar Systems (for air and/or marine incursions)
 - Aircraft systems (manned or unmanned)

Critical Emergency Supplies (SHSP and UASI)

Critical emergency supplies, such as shelf stable products, water, and medical equipment and supplies are an allowable expense under SHSP and UASI. Prior to the allocation of grant funds for stockpiling purposes, each state must have DHS/FEMA's approval of a five-year viable inventory management plan, which should include a distribution strategy and related sustainment costs if planned grant expenditure is over \$100,000.00.

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 as it relates to the purchase of critical emergency supplies under UASI. FEMA will establish guidelines and requirements for the purchase of these supplies under UASI and monitor development and status of the state's inventory management plan.

SAAAs (through their Emergency Management Office) are strongly encouraged to consult with their respective FEMA Regional Logistics Chief regarding disaster logistics-related issues. States are further encouraged to share their DHS/FEMA approved plan with local jurisdictions and tribes.

Construction and Renovation (SHSP and UASI)

Project construction using SHSP and UASI funds may not exceed the greater of \$1,000,000 or 15% of the grant award. For the purposes of the limitations on funding levels, communications towers are not considered construction. See guidance on communication towers below.

Written approval must be provided by DHS/FEMA prior to the use of any HSGP funds for construction or renovation. When applying for construction funds, recipients must submit evidence of approved zoning ordinances, architectural plans, and any other locally required planning permits. Additionally, recipients are required to submit a SF-424C form with budget detail citing the project costs.

Recipients using funds for construction projects must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). 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 like 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 online at <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Construction and Renovation (OPSG)

OPSG funds may not be used for any construction.

Communications Towers

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 using the guidelines in the Environmental and Historic Preservation (EHP) Supplement prior to submitting materials for EHP review. Completed EHP review materials for construction and communication tower projects must be submitted as soon as possible to get approved by the end of the POP. EHP review materials should be sent to gpdehpinfo@fema.dhs.gov.

Western Hemispheric Travel Initiative (SHSP)

In addition to the expenditures outlined above, SHSP funds may be used to support the implementation activities associated with the Western Hemisphere Travel Initiative (WHTI), including the issuance of WHTI-compliant tribal identification cards.

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 at <http://www.emap.org>.

28 C.F.R. Part 23 Guidance

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

Unallowable Costs (OPSG)

OPSG unallowable costs include costs associated with evidence collection, arrest processing, prosecution, and Traffic/DUI checkpoints, such as evidence documentation cameras, fingerprinting supplies, alcohol breathalyzers, portable work lights, traffic barricades, and similar law enforcement expenses. OPSG unallowable costs also include costs associated with staffing and general IT computing equipment and hardware, such as personal computers, faxes, copy machines, modems, etc. OPSG is not intended as a

hiring program. Therefore, applying funds toward hiring full-time or permanent sworn public safety officers is unallowable. OPSG funding shall not be used to supplant inherent routine patrols and law enforcement operations or activities not directly related to providing enhanced coordination between local and federal law enforcement agencies. Finally, construction and/or renovation costs are prohibited under OPSG. Applicants should refer to [IB No. 421b](#), or contact their FEMA HQ Program Analyst at (800) 368-6498 for guidance and clarification. Due to the nature of OPSG, exercise expenses are not allowable costs under OPSG.

Unallowable Costs (SHSP, UASI, and OPSG)

- Per FEMA policy, the purchase of weapons and weapons accessories, including ammunition, is not allowed with HSGP funds.
- Grant funds may not be used for the purchase of equipment not approved by DHS/FEMA. Grant funds must comply with [IB 426](#) and may not be used for the purchase of the following equipment: firearms; ammunition; grenade launchers; bayonets; or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.
- Unauthorized exercise-related costs include:
 - Reimbursement for the maintenance or wear and tear costs of general use vehicles (e.g., construction vehicles), medical supplies, and emergency response apparatus (e.g., fire trucks, ambulances).
 - Equipment that is purchased for permanent installation and/or use, beyond the scope of the conclusion of the exercise (e.g., electronic messaging sign).

Resources for Planning, Training, and Exercising (SHSP, UASI, and OPSG)

Planning Assistance

FEMA's National Preparedness Directorate (NPD) offers technical assistance (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 DHS/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 DHS/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 <http://www.fema.gov/national-incident-management-system/fema-technical-assistance-division>.

Training Information

Per DHS/FEMA Grant Programs Directorate [Information Bulletin 432](#), Review and Approval Requirements for Training Courses Funded Through Preparedness Grants, issued on July 19, 2018, states, territories, tribal entities, and high-risk urban areas are no longer required to request approval from FEMA for personnel to attend non-DHS FEMA training as long as the training is coordinated with and approved by the state, territory, tribal, or high-risk urban area Training Point of Contact (TPOC) and falls within the FEMA mission scope and the jurisdiction's Emergency Operations Plan (EOP). For additional information on review and approval requirements for training courses funded with preparedness grants, please refer to the following policy: <http://www.fema.gov/media-library/assets/documents/34856>.

DHS/FEMA will conduct periodic reviews of all state, local, territory, tribal entities, and high-risk urban area training funded by DHS/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. For further information on developing courses using the instructional design methodology and tools that can facilitate the process, SAAs and TPOCs are encouraged to review the [NTED Responder Training Development Center \(RTDC\)](#) website.

DHS/FEMA/National Training and Education Division (NTED) Provided Training

Trainings include programs or courses developed for and delivered by institutions and organizations funded by DHS/FEMA/NTED. This includes CDP and NTED's Training Partner Programs, including CTG, NDPC, RDPC, and other partners.

NTED's National Preparedness Course Catalog

This online searchable catalog features a compilation of courses managed by the three primary FEMA training organizations: the CDP, EMI, and NTED. 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, state, local, territorial, and tribal audiences. All courses have been approved through NTED's course review and approval process. The catalog can be accessed at <http://www.firstrespondertraining.gov>.

Training Not Provided by DHS/FEMA

These trainings include courses that are either State-sponsored or Federal sponsored (non-DHS/FEMA), coordinated and approved by the SAA or their designated TPOC, and fall within the DHS/FEMA mission scope to prepare SLTT personnel to prevent, protect against, mitigate, respond to, and recover from acts of terrorism or catastrophic events.

- *State Sponsored Courses.* These courses are developed for and/or delivered by institutions or organizations other than federal entities or DHS/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, respond to, and recover from acts of terrorism or catastrophic events. In addition, states, territories, tribes, and high-risk urban areas are encouraged to incorporate the private sector in government-sponsored training and exercises.

Additional information on both DHS/FEMA provided training and other Federal and State training can be found at <http://www.firstrespondertraining.gov>.

Training Information Reporting System ("Web-Forms")

Web-Forms is an electronic data management system built to assist SAA TPOCs 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 HSGP 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 DHS/FEMA Toolkit located at <https://www.firstrespondertraining.gov/frt/> to support recipients in their own tracking of training deliveries.

Exercise Information

Recipients that use HSGP funds to conduct an exercise(s) are encouraged to complete a progressive exercise series. Exercises conducted by states and high-risk urban areas may be used to fulfill similar exercise requirements required by other grant programs. Recipients are encouraged to invite representatives/planners involved with other Federally mandated or private exercise activities. States and high-risk urban areas are encouraged to share, at a minimum, the multi-year training and exercise schedule with those departments, agencies, and organizations included in the plan.

- *Validating Capabilities.* Exercises examine and validate capabilities-based planning across the Prevention, Protection, Mitigation, Response, and Recovery mission areas. The extensive engagement of the whole community, including but not limited to examining the needs and requirements for individuals with disabilities, individuals with limited English proficiency, and others with access and functional needs, is essential to the development of an effective and comprehensive exercise program. Exercises are designed to be progressive – increasing in scope and complexity and drawing upon results and outcomes from prior exercises and real-world incidents – to challenge participating communities. Consistent with Homeland Security Exercise and Evaluation Program guidance and tools, the National Exercise Program (NEP) serves as the principal exercise mechanism for examining national preparedness and measuring readiness. Exercises should align with priorities and capabilities identified in a multi-year TEP.
- *Special Event Planning.* If a state or high-risk urban area will be hosting a special event (e.g., Super Bowl, G-8 Summit), the special event planning should be considered as a training or exercise activity for the multi-year TEP. States must include all confirmed or planned special events in the multi-year TEP. The state or high-risk urban area may plan to use SHSP or UASI funding to finance training and exercise activities in preparation for those events. States and high-risk urban areas should also consider exercises at major venues (e.g., arenas, convention centers) that focus on evacuations, communications, and command and control.
- *Regional Exercises.* States should also anticipate participating in at least one regional exercise annually.
- *Role of Non-Governmental Entities in Exercises.* Non-governmental participation in all levels of exercises is strongly encouraged. Leaders from non-governmental entities should be included in the planning, design, and evaluation of an exercise. SLTT jurisdictions are encouraged to develop exercises that test the integration and use of resources provided by non-governmental entities, defined as the private sector and private non-profit, faith-based, and community organizations. Participation in exercises should be coordinated with local Citizen Corps Whole Community Council(s) or their equivalents and other partner agencies.

OPSG Operations Order Template and Instructions

Operations Order Template Instructions

To access the OPSG Operations Order Template:

- Find the Homeland Security Grant Program posting via the search function on grants.gov
- Select the Related Documents tab on the posting
- Click on the OPSG Operations Order Template and fill out all sections of the template

Executive Summary Overview

Operations Order Executive Summary must:

- Identify the organization name, point of contact, committees, and other structures accountable for implementing OPSG in the jurisdiction (typically this will be a program lead or manager overseeing operations and individuals assigned to that agency).
- Describe how federal and SLTT law enforcement agencies will work together to establish and enhance coordination and collaboration on border security issues.

Budget Requirements Overview

Operations Order Detailed Annual Budget must:

- Explain how costs and expenses were estimated.
- Provide a narrative justification for costs and expenses. Supporting tables describing cost and expense elements (e.g., equipment, fuel, vehicle maintenance costs) may be included.

Submission Requirements

Operations Orders must meet the following submission requirements:

- Must be submitted as an Adobe PDF document.
- All documents submitted must use the unique identifier created by the OPSG data management system from the original associated operation order.
- Applicable OPSG sector representatives must coordinate with the SAA and OPSG participants to submit an accurate inventory of all specified OPSG purchased property with each Operations Order/FRAGO.

Due to the competitive nature of this program, separate attachments will neither be accepted nor reviewed.

OPSG Operational Guidance

This section provides operational guidance to OPSG applicants on the development of a concept of operations and 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, 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
- 3) Intelligence Collection 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 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, statues, 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 *INA*). Participation in the grant does not grant participants the power to operate outside of their own jurisdictional boundaries.

Concept of Operations and Campaign Planning

(Post-Allocation Announcement/Pre-Award)

The overarching operational cycle involves three stages: 1) application; and 2) concept of operations to formulate a Campaign Plan, which are all developed by the IPT. All Operations Orders: Concept of Operations (CONOPS), Operation Orders (OO) or Campaign Plans and Fragmentary Orders (FRAGOs) shall be submitted through the CBP Stonegarden Data Management System. All OPSG grant Application packages shall be submitted to the SAA for entry into [Grants.gov](https://www.grants.gov).

Application: Please refer to the current fiscal year's HSGP NOFO and relevant information in this manual.

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 PRICE Act waiver request must be submitted in accordance with the policy initially outlined in [IB 379: Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding. 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)(i), 200.407.

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

Operational Execution

In the event that changes or additional funding requests to the original operational order must be made, a Fragmentary Order (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 state, local, tribal, and territorial 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, but the 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 operations order in the corresponding folder in the CBP Stonegarden Data Management System.

Reporting Procedures

Participation in OPSG requires accurate, consistent, and timely reporting of how funds are used, and how the state, local and tribal 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 state, local, and tribal 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 link for the current fiscal year HSGP NOFO on FEMA's preparedness grants page (<https://www.fema.gov/homeland-security-grant-program>) 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 After Action Reports to USBP sectors within 10 days of closing the operational POP for that funding year. The After-Action Report (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.

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 Integrated Planning Team'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 DHS/FEMA
 - 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, 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 state, local, and tribal agencies in the proper format and within the established timeframes

- Providing instruction, when possible, to state, local, and tribal 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
- 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 state, local or tribal 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 Integrated Planning team to develop an individualized campaign plan that covers the length of the grant performance period;
- Work within the Integrated Planning team 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 Operations Section;
 - Conduct operations on an as-needed basis 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 Operation Stonegarden 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 urban areas;
 - Request instruction and information from the SAA, when applicable, and/or Border Patrol and other Federal law enforcement agencies regarding techniques, methods, and trends used by transnational criminal organizations in the area; and
 - Provide the SAA and Border Patrol 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.
 - 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;
- Acts 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 DHS/FEMA;
- Generate biannual reports to DHS/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; and
- Conduct audits of the program to ensure that the subrecipients are following program guidance.
- Assist as required with the coordination, management, and operational aspects of the grant.

Definitions (OPSG only)

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:

- 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; and
- For which prosecution would serve established border security goals as outlined by the CBP for a whole of community approach.

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

Concept of Operations (CONOP): A written statement that clearly and concisely expresses what the State, local, or tribal commander intends to accomplish and how it will be done using available resources (and funding). It is also the operational equivalent of the OPSG grant application.

Fragmentary Order (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)(i). 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 with whom OPSG subrecipients provide funding to support border security operations.

Integrated Planning Team: Group that coordinates on all aspects of OPSG application, planning, and debriefings.

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 (OO): A formal description of the action to be taken to accomplish or satisfy a CONOP, Campaign Plan, or FRAGO. The OO 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 utilized by first responder personnel in an emergency situation 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 tribe 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.

HSGP Supplemental Material

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. 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 hyperlinks to information on various subjects and policies that are relevant to the mission and intent of the DHS/FEMA and its preparedness grant programs.

Chemical, Biological, Radiological, and Nuclear (CBRN) 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. CWMD offers THIRA Technical Assistance for CBRN threats to provide guidance to SLTT partners seeking to build or sustain CBRN detection and response capabilities. For more information or assistance, please contact CWMD-THIRA@hq.dhs.gov.

National Information Exchange Model (NIEM)

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 conformance rules. Go to <https://niem.gov/> for guidance on how to utilize DHS/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 Emergency Management domain has an inclusive governance structure that includes federal, state, local, industry, and, where necessary, international partnerships. The NIEM Emergency Management domain is committed to community support via technical assistance and NIEM training. For more information on the NIEM Emergency Management domain, to request training or technical assistance or to just get involved, go to <https://niem.gov/EM>.

Integrated Public Alert and Warning System (IPAWS)

The current IPAWS Supplemental Guidance on Public Alert and Warning provides guidance on eligible public alert and warning activities and equipment standards for prospective SLTT recipients. The intent of this document is to promote consistency in policy across federal grant programs and to ensure compatibility among federally-funded projects. For more information on the IPAWS, go to <https://www.fema.gov/informational-materials>.

Homeland Security Information Network (HSIN)

HSIN is a user-driven, web-based, information sharing platform that connects all homeland security professionals including the DHS and its federal, state, local, tribal, territorial, 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 at <http://www.dhs.gov/hsin-hsgp-guidance>.

State, Local, Tribal and Territorial (SLTT) Cybersecurity Engagement Program

The DHS CS&C, within CISA, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C works to prevent or minimize disruptions to critical information infrastructure to protect the public, the economy, and government services. CS&C

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 CS&C 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 of the DHS CS&C resources available to support SLTT governments is available at <https://www.us-cert.gov/ccubedvp>.

Regional Resiliency Assessment Program (RRAP)

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 the 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 <https://www.dhs.gov/regional-resiliency-assessment-program>.

Law Enforcement Support Office, or 1033 Program

The Law Enforcement Support Office (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 by 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 gamut of items used by America’s military — clothing and 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, please visit <http://www.dla.mil/DispositionServices/Offers/Reutilization/LawEnforcement.aspx>.

Fusion Center Performance Measures

Reference Number	Performance Measures
2020.1	Percentage of federal Information Intelligence Reports (IIRs) originating from fusion center information that address a specific Intelligence Community need
2020.2	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 gaps; or helped to define an issue or target).

2020.3	Number of Suspicious Reports (SAR) vetted and submitted by fusion centers that result in the initiation or enhancement of an investigation by the Federal Bureau of Investigation (FBI)
2020.4	Number of SAR vetted and submitted by fusion centers that involve an individual on the Watchlist
2020.5	Percentage of Requests for Information (RFIs) from the Terrorist Screening Center (TSC) for which fusion centers provided information for a TSC case file
2020.6	Percentage of I&A Watchlist nominations that were initiated or updated existing case files based on information provided by fusion centers
2020.7	Number of distributable analytic products co-authored by one or more fusion centers and/or federal agencies
2020.8	Percentage of fusion center distributable analytic products that address Homeland Security topics
2020.9	Percentage of fusion center distributable analytic products that address state/local customer information needs
2020.10	Percentage of key customers reporting that fusion center products are relevant
2020.11	Percentage of key customers reporting that fusion center services are relevant
2020.12	Percentage of key customers reporting that fusion center products are timely for mission needs
2020.13	Percentage of key customers reporting that fusion center services are timely for mission needs
2020.14	Percentage of key customers reporting that fusion center products influenced their decision making related to threat response activities within their AOR
2020.15	Percentage of key customers reporting that fusion center services influenced their decision making related to threat response activities within their AOR
2020.16	Percentage of key customers reporting that fusion center products resulted in increased situational awareness of threats within their AOR
2020.17	Percentage of key customers reporting that fusion center services resulted in increased situational awareness of threats within their AOR
2020.18	Number of tips and leads vetted by the fusion center
2020.19	Number of tips and leads vetted by the fusion center that were provided to other F/SLTT agencies for follow up action
2020.20	Number of responses to RFIs from all sources
2020.21	Number of situational awareness products developed and disseminated by fusion centers
2020.22	Number of case support and/or tactical products developed and disseminated by fusion centers
2020.23	Percentage of federally designated special events in which fusion centers played a direct role
2020.24	Percentage of federally declared disasters in which fusion centers played a direct role

Supplemental Emergency Communications Guidance

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 a number of 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 the National Incident Management System (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 Communications Interoperability Plan (SCIP), Tactical Interoperability Communications Plan (TICP), FEMA Regional Emergency Communications Plan (RECP)), project coordination, and technical standards for emergency communications technologies. 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, tribes, 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.

In addition, DHS/FEMA formally recognizes several Statewide emergency communications governance bodies (e.g., Statewide Interoperability Coordinator (SWIC), Statewide Interoperability Governing Body (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, grantees 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, DHS/FEMA requires applicants to coordinate projects with national level emergency communications coordination bodies, such as the National Committee of Statewide Interoperability Coordinators (NCSWIC) and the Regional Emergency Communications Coordination Working Groups (RECCWGs). The NCSWIC promotes and coordinates state level activities designed to ensure the highest level of public safety communications across the nation. RECCWGs are congressionally mandated planning and coordination bodies located in each FEMA Region that provide a collaborative forum to assess and address the survivability, sustainability, operability, and interoperability of emergency communications systems at all levels of government. Grant-funded investments that are coordinated with these bodies will help ensure that Federally funded emergency communications investments are interoperable and support national policies.

Resilient Communications Guidance

Nothing better demonstrates a modern nation than its ability to effectively communicate. 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 HSGP funding for communications investments are encouraged to work with State emergency management agencies, SWICs, SIGBs, and appropriate stakeholders at the regional, state, local, territorial, and tribal levels to:

- 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, grantees 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
 - Maintain spares for designated critical communication systems
 - Work with commercial suppliers to remediate communication Single Points of Failure
- All communications system owners are encouraged to address the following issues:
 - Integrate communications needs into continuity planning efforts by incorporating 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
- Consider Electromagnetic Pulse (EMP) protective measures for communications systems where practical.

DHS/FEMA Communications Support Services

DHS's Cybersecurity and Infrastructure Agency's (CISA) Emergency Communications Division (ECD) and FEMA offer a variety of technical assistance 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/FEMA support services is provided below. Grant recipients are encouraged to refer to the respective websites for additional information.

DHS OEC Support:

To assist in these efforts, DHS established the OEC, which assists agencies through a myriad of services, including direct technical assistance (TA) and training provided at no cost to the jurisdiction. The TA offerings include (but are not limited to):

- Enhanced Governance Structure – Enhanced SCIP Workshop
- Communications Unit (COMU) Policy and Planning Development at the State and County Level
- COMU Assistance under EMAC
- Next Generation 9-1-1 (NG9-1-1)
- Alerts and Warnings
- Continuity Planning

Information on these services is available at <https://www.dhs.gov/ictapscip-resources> and <https://www.dhs.gov/oec-technical-assistance-program>.

FEMA Disaster Emergency Communications Division (DEC) Support:

DEC has developed State Communications Annexes for all of the 56 States and territories. DEC provides technical assistance, coordinated through the FEMA Region's Regional Emergency Communications Coordinator (RECC) in scheduling with the State and Territories major updates to the Annexes. Major updates are scheduled on a 3 to 5-year cycle. FEMA DEC supports the major update with a team of communications and emergency management specialists that facilitate a process of interaction with state representatives. This process is coordinated through the SWICC or State designated representative. All documentation is the responsibility of the FEMA support team and validated through State interaction.

Minor yearly updates to the State Annexes is accomplished through the RECCWG process. FEMA DEC support staff, working in coordination with the region-specific RECC, incorporate pertinent update information provided by state and local representatives. Additionally, operational information identified through exercises and incident response activities is a source of update data. The FEMA RECC, with the support of the DEC team, is responsible for maintaining the State Annexes — changes and modifications to the Annexes are validated with the State through RECC coordination with the SWIC or designated State representative.

FEMA National Preparedness Directorate (NPD) Support:

NPD provides training, exercises, and technical assistance to SLTT stakeholders that support operational and emergency communications. Descriptions and resources specific to operational communication are available on FEMA's website (<https://www.fema.gov/core-capability-development-sheets>) 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 <https://www.firstrespondertraining.gov/frt/>.
- Example capability targets to complete a Threat and Hazard Identification and Risk Assessment
 - Help in developing targets can be requested at FEMA-SPR@fema.dhs.gov
- Resources types that support operational communications
 - Additional resource types and position qualifications can be found at <https://www.fema.gov/preparedness-checklists-toolkits>.
- Tools to validate capabilities through exercises
 - Technical assistance and support from subject matter experts can be requested through www.fema.gov/national-exercise-program.

FEMA National Continuity Programs (NCP) Support:

NCP's support services focus on holistic continuity planning, of which communications continuity is an important component. Currently, continuity communications training and technical assistance is limited to the FEMA National Radio System (FNARS) and the Integrated Public Alert and Warning System (IPAWS) and is delivered either on an ad hoc basis at the request of the state entity, through a FEMA Region, or via a requirement for terms of use. Entities interested in NCP support services should contact FEMA-CGC@fema.dhs.gov or consult NCP's Continuity Resources Toolkit webpage at <https://www.fema.gov/continuity-resource-toolkit>.

Program Appendix B: Tribal Homeland Security Grant Program (THSGP)

Alignment of THSGP to the National Preparedness System

The THSGP plays an important role in the implementation of the Goal by supporting the building, sustainment, and delivery of the core capabilities. The core capabilities are essential for the execution of critical tasks for each of the five mission areas outlined in the Goal. Delivering core capabilities requires the combined effort of the whole community, rather than the exclusive effort of any single organization or level of government. THSGP allowable costs support efforts to build and sustain core capabilities across the prevention, protection, mitigation, response, and recovery mission areas described in the Goal.

Particular emphasis in THSGP will be placed on capabilities that address the greatest risks to the security and resilience of tribal communities and the United States and that provide a clear nexus to preventing acts of terrorism. Funding will support deployable assets that can be utilized through automatic assistance and mutual aid agreements. THSGP 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; and/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.

To support building, sustaining, and delivering these core capabilities, recipients will use the components of the National Preparedness System, which include: 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: <http://www.fema.gov/national-preparedness-system>.

DHS/FEMA requires recipients to prioritize grant funding to demonstrate how investments support identified national priorities and closing capability gaps or sustaining capabilities identified in the THIRA/SPR process. Recipients are also expected to consider national areas for improvement identified in the most recent National Preparedness Report as they relate to terrorism preparedness. They include cybersecurity, economic recovery, housing, infrastructure systems, natural and cultural resources, and supply chain integrity and security. Addressing these areas for improvement will enhance preparedness nationwide. Minimum funding amounts are not prescribed by the Department for these priorities; however, recipients are expected to support state, local, regional, and national efforts in achieving the desired outcomes of these priorities.

Reporting on the Implementation of the National Preparedness System

By December 31, 2020, THSGP recipients are required to complete a THIRA/SPR that addresses all 32 core capabilities and is compliant with Comprehensive Preparedness Guide (CPG) 201, Third Edition. Specific guidance on the requirements for each core capability will be forthcoming in 2020, as some core capabilities have fewer reporting requirements than others.

THSGP recipients must complete every step of the THIRA/SPR for the following eight core capabilities: Cybersecurity; Infrastructure Systems; Mass Care Services; Mass Search and Rescue Operations; On-scene Security, Protection, and Law Enforcement; Operational Communications; Operational Coordination; and Public Information and Warning. For the remaining 24 core capabilities, THSGP recipients are only required to indicate planning, organization, equipment, training, and exercise gaps in functional areas related to those capabilities. THSGP recipients may optionally complete additional portions of the THIRA/SPR for these 24 core capabilities.

Beginning in 2020, THSGP recipients will also be required to respond to a series of planning-related questions as part of the THIRA/SPR. THSGP recipients are required to submit a THIRA every three (3) years to establish a consistent baseline for assessment. While the THIRA will be only required every three years, THSGP recipients will continue to be required to submit an SPR annually. For additional guidance on the THIRA/SPR, please refer to the [Comprehensive Preparedness Guide \(CPG\) 201, Third Edition](#). Recipients must align THSGP grant investments in building and sustaining capabilities with closing capability gaps and/or sustaining capabilities they identified in their THIRA and SPR.

Reporting Requirements

- THSGP recipients must submit their THIRA and SPR through the Unified Reporting Tool (URT) on [Prep Toolkit](#) no later than December 31 of the applicable year (every three years for THIRA and each year for SPR). FY20 THSGP Recipients must also update their SPR inputs in 2021 and 2022.
- Please contact FEMA-SPR@fema.dhs.gov if you have questions.
- In each THSGP recipient's BSIR, as part of programmatic monitoring, recipients will be required to describe how investments support closing capability gaps or sustaining capabilities identified in the THIRA/SPR. THSGP recipients will, on a project-by-project basis, check one of the following:
 - Building a capability with THSGP funding; or
 - Sustaining a capability with THSGP funding.

National Incident Management System (NIMS) Implementation

Recipients receiving THSGP funding are required to implement the National Incident Management System (NIMS). 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. THSGP recipients must utilize standardized resource management concepts such as typing, credentialing, and inventorying resources that facilitates the effective identification, dispatch, deployment, tracking and recovery of their resources.

Reporting Requirements

Recipients will use the URT to report NIMS implementation.

Planning to Deliver Capabilities

Recipients shall develop and maintain a jurisdiction wide, all threats and hazards EOPs consistent with CPG 101 Version 2.0 (v2). Recipients must submit an EOP once during the period of performance.

Reporting Requirements

Recipients report EOP compliance with Developing and Maintaining Emergency Operations Plans CPG 101 v2 in the URT.

National Exercise Program

The National Exercise Program (NEP) is a two-year cycle of exercises across the nation that examines and 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 affords exercise sponsors with the opportunity to receive exercise design and delivery assistance, tools and resources, enhanced coordination, and the ability to directly influence and inform policy, resource allocation, and preparedness programs assistance from seasoned and innovative Federal Emergency Managers. If you have any questions or would like to nominate your exercise to be a part of the NEP, please visit the NEP website at: <https://www.fema.gov/national-exercise-program> or reach out to the National Exercise Program directly at NEP@fema.dhs.gov.

Validating Capabilities

All recipients will develop and maintain a progressive exercise program consistent with Homeland Security Exercise and Evaluation Program (HSEEP) guidance in support of the National Exercise Program (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.

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 Training and Exercise Plan (TEP) or an Integrated Preparedness Plan (IPP). Information related to TEPs and Training and Exercise Planning Workshops (TEPWs), as well as information about IPPs and Integrated Preparedness Planning Workshops (IPPWs), can be found on the HSEEP website at <https://www.fema.gov/HSEEP> and <https://preptoolkit.fema.gov/>.

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 at: <https://www.fema.gov/national-exercise-program> or reach out to the National Exercise Program directly at NEP@fema.dhs.gov.

Reporting

- Recipients must have a current multi-year TEP or IPP that identifies preparedness priorities and activities. The current multi-year TEP or IPP must be submitted to hseep@fema.dhs.gov before January 31 of each year.
 - Recipients are encouraged to enter their exercise information in the Preparedness Toolkit at <https://preptoolkit.fema.gov/>.
- Recipients must submit After-Action Report (AAR)/Improvement Plans (IPs) to hseep@fema.dhs.gov and indicate which fiscal year's funds were used (if applicable).
- Submission of AAR/IPs must be no later than December 31 of each year. Recipients are encouraged to submit AAR/IPs within 90 days after completion of the single exercise or progressive series.
 - Recipients are encouraged to submit AAR/IPs reflecting table top exercises which validate critical plans or those reflecting large-scale functional or full-scale exercises which took place at the state, territorial, tribal, or UASI level. Recipients are discouraged from submitting AAR/IPs specific to local jurisdictions which reflect drills.
 - If a recipient endures a significant real-world incident during the calendar year, they can submit the AAR from that event in place of one or more of the exercises AARs depending on the size and scale of the incident. Jurisdictions submitting real world AARs should include a request to do so with the AAR submission to hseep@fema.dhs.gov.
 - Recipients can access a sample AAR/IP template at <https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning>.

THSGP Funding Guidelines

Recipients and subrecipients 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. In administering a THSGP grant award, recipients must comply with the following general requirements:

THSGP Priorities

See the annual THSGP NOFO.

Allowable Costs

Management and Administration (M&A)

M&A activities are those defined as directly relating to the management and administration of THSGP funds, such as financial management and monitoring. Recipients may use up to 5% of the amount of the award for M&A, and where applicable, subrecipients may use up to 5% for M&A of the amount they receive. Reasonable costs of grant management training are also allowable.

Indirect (Facilities and Administrative [F&A]) Costs

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their

proposal at the time of application. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal.

Allowable Direct Costs

The following pages outline global allowable costs guidance specifically applicable to THSGP. Allowable activities made in support of the national priorities, as well as other capability-enhancing projects must fall into the categories of planning, organization, equipment, training, or exercises (POETE). Additional detail about each of these allowable expense categories, as well as sections on additional activities including explicitly unallowable costs is provided. In general, recipients should consult their FEMA Program Analyst prior to implementing any investment to ensure that it clearly meets the allowable expense criteria established by the guidance.

Recipients are encouraged to use grant funds for evaluating grant-funded project effectiveness and return on investment aligned to the relevant POETE element, and FEMA encourages grant recipients to provide the results of that analysis to FEMA.

Planning

Planning efforts can include prioritizing needs, updating preparedness strategies, and allocating resources across stakeholder groups (e.g., law enforcement, fire, EMS, health care systems, public health, behavioral health, public works, rural water associations, agriculture, information technology, emergency communications, and the general public, including people with disabilities) and levels of government. Planning provides a methodical way to engage the whole community in thinking through the life cycle of potential crises, determining required capabilities, and establishing a framework for roles and responsibilities. Planning must include participation from all stakeholders in the community who are able to contribute critical perspectives and may have a role in executing the plan. Planning should be flexible enough to address incidents of varying types and magnitudes.

Planning activities should focus on the prevention, protection, mitigation, response, and recovery mission areas outlined in the Goal. All jurisdictions are encouraged to work with Citizen Corps Whole Community Councils, nongovernmental entities, and the general public in planning activities. Whole community planning should integrate program design and delivery practices that ensure representation and services for under-represented diverse populations that may be more impacted by disasters including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations. Recipients must use the CPG 101 v2 in order to develop robust and effective plans.

For additional planning and resource information, please see:
http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf
<http://www.ready.gov/citizen-corps>
<http://www.fema.gov/community-emergency-response-teams>
www.ready.gov/kids
<http://www.fema.gov/media-library/assets/documents/94775>.
<http://www.fema.gov/pdf/recoveryframework/ndrf.pdf>

Continuity of Operations

DHS/FEMA is designated as the Department of Homeland Security's lead agency for managing the nation's Continuity Program. To support this role, FEMA provides direction and guidance to assist in developing capabilities for continuing federal and SLTT government jurisdictions and private sector organizations' essential functions across a broad spectrum of emergencies.

Presidential Policy Directive 40, the National Continuity Policy Implementation Plan (NCPIP), Federal Continuity Directive 1 (FCD 1), Federal Continuity Directive 2 (FCD 2), and Continuity Guidance Circular (CGC) outline continuity requirements for agencies and organizations and provide guidance, methodology, and checklists. For additional information on continuity programs, guidance, and directives, visit <http://www.fema.gov/guidance-directives> and <https://www.fema.gov/national-continuity-programs> or contact a [Regional Continuity Manager](#). Please note, the Continuity Guidance Circular (2018) supersedes Continuity Guidance Circular-1, *Continuity Guidance for Non-Federal Governments* (July 2013), and Continuity Guidance Circular-2, *Continuity Guidance for Non-Federal Governments: Mission Essential Function Identification Process* (Oct. 2013). U.S. Dep't of Homeland Security, *Continuity Guidance Circular* at 8 (Feb. 2018).

Organization

Recipients may use grant funds for organization activities:

- Organizational activities may include, paying salaries and benefits for personnel, including individuals employed to serve as qualified intelligence analysts. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.
- Other organization activities may include implementing standardized resource management concepts such as typing, inventorying, organizing, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident.

Equipment

The 21 allowable prevention, protection, mitigation, response, and recovery equipment categories and equipment standards for THSGP are listed on the web-based version of the Authorized Equipment List (AEL) available at <https://www.fema.gov/authorized-equipment-list>. Unless otherwise stated, equipment must meet all mandatory regulatory and DHS-adopted standards to be eligible for purchase using these funds. In addition, recipients and subrecipients, as applicable, agencies will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

Grant funds must comply with [Information Bulletin \(IB\) 426](#) and may not be used for the purchase of the following unallowable equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed. Recipients should analyze the costs and benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 C.F.R. Part 200, including 2 C.F.R. §§ 200.310, 200.313, and 200.316.

Requirements for Small Unmanned Aircraft System

All requests to purchase Small Unmanned Aircraft System (SUAS) devices must also comply with [IB 426](#) and must include the policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties maintained by the jurisdiction that will purchase, take title to, or otherwise use the SUAS device.

Training and Exercises

Tribes are strongly encouraged to use THSGP funds to develop or maintain a homeland security training program. Allowable training-related costs under the THSGP include the establishment, support, conduct, and attendance of training specifically identified under the THSGP or in conjunction with emergency preparedness training by other federal agencies (e.g., the Department of Health and Human Services or

the Department of Transportation). Training conducted using THSGP funds should address a performance gap identified through an assessment or contribute to building a capability that will be evaluated through a formal exercise. Exercises should be used to provide the opportunity to demonstrate and validate skills learned in training, as well as to identify training gaps. Any training or training gaps evaluated through a formal exercise, including those for vulnerable populations including children, the elderly, pregnant women, and individuals with disabilities or access and functional needs should be identified in an AAR/IP.

All training and exercises conducted with THSGP funds should support the development and testing of the jurisdiction's Emergency Operations Plan (EOP), consistent with the priorities in the National Preparedness System. Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analysis, Design, Development, Implement, and Evaluate (ADDIE) model of instruction design, available with additional training information at <https://www.firstrespondertraining.gov>.

DHS/FEMA supports and encourages the coordination of all emergency preparedness training towards the achievement of the Goal. To this end, DHS/FEMA supports the establishment of a Tribal Training Point of Contact (TTPOC). The role of the TTPOC is to coordinate the tribes' training needs and activities with DHS/FEMA and DHS/FEMA's federal training partners and holds the same authority and roles that State training points of contact serve within SAAs nationwide. DHS/FEMA will coordinate with Tribal Training Officers (TTOs) as it relates to FEMA training when notified by recipients.

Per DHS/FEMA Grant Programs Directorate [Information Bulletin 432](#), Review and Approval Requirements for Training Courses Funded Through Preparedness Grants, issued on July 19, 2018, states, territories, tribal entities, and high-risk urban areas are no longer required to request approval from FEMA for personnel to attend non-DHS FEMA training as long as the training is coordinated with and approved by the state, territory, tribal, or high-risk urban area Training Point of Contact (TPOC) and falls within the FEMA mission scope and the jurisdiction's Emergency Operations Plan (EOP). For additional information on review and approval requirements for training courses funded with preparedness grants, please refer to the following policy: <http://www.fema.gov/media-library/assets/documents/34856>.

DHS/FEMA/National Training and Education Division (NTED) Provided Training

Trainings include programs or courses developed for and delivered by institutions and organizations funded by DHS/FEMA/NTED. This includes the Center for Domestic Preparedness (CDP), the Emergency Management Institute (EMI), and NTED's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), and other partners.

NTED's National Preparedness Course Catalog

This online searchable catalog features a compilation of courses managed by the three primary FEMA training organizations: the CDP, EMI, and NTED. 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, state, local, territorial, and tribal audiences. All courses have been approved through NTED's course review and approval process. The catalog can be accessed at <http://www.firstrespondertraining.gov>.

Training Not Provided by DHS/FEMA

These trainings include courses that are either State sponsored or Federal sponsored (non-DHS/FEMA), coordinated and approved by the SAA or their designated TPOC, and fall within the DHS/FEMA mission scope to prepare SLTT personnel to prevent, protect against, mitigate, respond to, and recover from acts of terrorism or catastrophic events.

- **State Sponsored Courses.** These courses are developed for and/or delivered by institutions or organizations other than Federal entities or DHS/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, respond to, and recover from acts of terrorism or catastrophic events. In addition, states, territories, tribes, and urban areas are encouraged to incorporate the private sector in government-sponsored training and exercises.

Additional information on both DHS/FEMA provided training and other Federal and State training can be found at <http://www.firstrespondertraining.gov>.

Training Information Reporting System (“Web-Forms”)

Web-Forms is an electronic data management system built to assist SAAs, designated TPOCs, 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 HSGP 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 FY 2020 THSGP. However, the system remains available and can be accessed through the DHS/FEMA Toolkit located at <https://www.firstrespondertraining.gov/frt/> to support recipients in their own tracking of training deliveries.

Exercises

For additional information on conducting exercises under THSGP, please refer to the earlier section in this appendix on the NEP.

Personnel Activities

Personnel hiring, overtime, and backfill expenses are permitted under this grant in order to perform allowable THSGP planning, training, exercise, and equipment activities.

Not more than 50% of total THSGP funds may be used for personnel activities as directed by the *Homeland Security Act of 2002*, as amended by the *Personnel Reimbursement for Intelligence Cooperation and Enhancement (PRICE) of Homeland Security Act* (Pub. L. No. 110-412) (6 U.S.C. § 609(b)(2)(A)). This 50% cap may be waived, however, per 6 U.S.C. § 609(b)(2)(B). For further details, THSGP recipients should refer to [Information Bulletin No. 421b](#), or contact their FEMA HQ Program Analyst. THSGP funds may not be used to support the hiring of any personnel for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities.

Construction and Renovation

Construction projects are only permitted where they will assist the recipient to achieve target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism, including through the alteration or remodeling of existing buildings for the purpose of making them secure against acts of terrorism. THSGP funding may not be used for construction and renovation projects without prior written approval from FEMA. All recipients of THSGP funds must request and receive approval from FEMA before any THSGP funds are used for any construction or renovation. Additionally, recipients are required to submit an SF-424C Form containing budget detail citing the construction project costs and an SF-424D Form for standard assurances for the construction project. The total cost of any construction or renovation paid for using THSGP funds may not exceed the greater amount of \$1,000,000 or 15% of the THSGP award.

THSGP recipients using funds for construction projects must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). 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. Additional information regarding compliance with the *Davis-Bacon Act*, including Department of Labor (DOL) wage determinations, is available from the following website: <http://www.dol.gov/whd/govcontracts/dbra.htm>.

Communications Towers

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

When applying for funds to construct communication towers, recipients and subrecipients must submit evidence that the Federal Communication Commission's Section 106 review process has been completed and submit all documentation resulting from that review to DHS/FEMA prior to submitting materials for EHP review. Recipients and subrecipients are also 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 Tribal Historic Preservation Office to identify potential historic preservation issues and to discuss the potential for project effects; compliance with all State and EHP laws and requirements). Projects for which 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 Program Analyst within six months of the recipient's receipt of the award. Completed EHP review materials for construction and communication tower projects must be submitted no later than 12 months before the end of the period of performance. EHP review materials should be sent to gpdehpinfo@fema.gov.

Multiple Purpose or Dual-Use of Funds

Many activities that support the achievement of target capabilities related to terrorism preparedness may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. *See* 6 U.S.C. § 609(c). However, all THSGP-funded projects must assist recipients and subrecipients in achieving target capabilities related to preventing, preparing for, protecting against, or responding to acts of terrorism.

Whole Community Preparedness

In addition to the Citizen Corps Whole Community Councils and CERT programs mentioned above, the following preparedness programs are allowable expenses:

- **Youth Preparedness Resources** to support practitioners as they create and run programs in their communities are available at www.ready.gov/kids. The interactive website is a one-stop shop with search features, tools, and resources for parents, caregivers, and educators to help engage kids and young people on emergency and disaster preparedness. Site visitors can find information, programs, curricula, and games and activities that engage and teach youth and their families to be prepared. Ready.gov/kids also has resources to support the integration and implementation of children’s disaster-related needs into preparedness, planning, response and recovery efforts initiated by state, local, territorial and tribal governments, and stakeholders responsible for the temporary care of children.

Other Allowable Costs

Maintenance and Sustainment

The use of FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted, as described in FEMA Policy FP 205-402-125-1, *Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants*, located at: <http://www.fema.gov/media-library/assets/documents/32474>.

Grant funds are intended to support the National Preparedness Goal and fund projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in [IB 379: Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#) allows for the expansion of eligible maintenance and sustainment costs which must be in (1) direct support of existing capabilities, (2) must be an otherwise allowable expenditure under the applicable grant program, and (3) be tied to one of the core capabilities in the five mission areas outlined in the Goal. Additionally, eligible costs must also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant money or any other source of funding other than DHS/FEMA preparedness grant program dollars.

Critical Emergency Supplies

In furtherance of DHS’s mission, critical emergency supplies, such as shelf-stable food products, water, and basic medical supplies are an allowable expense under THSGP. Prior to allocating grant funds for stockpiling purposes, each Tribe must have FEMA’s approval of a five-year viable inventory management plan, an effective distribution strategy, and related sustainment costs if the planned grant expenditure is over \$100,000.

The inventory management plan and distribution strategy, to include sustainment costs, will be developed and monitored by FEMA. FEMA will provide program oversight and technical assistance as it relates to the purchase of critical emergency supplies under THSGP. FEMA will establish guidelines and requirements for the purchase of these supplies under THSGP and monitor development and status of the Tribe’s inventory management plan and distribution strategy. Linkages between specific projects undertaken with THSGP funds and strategic goals and objectives will be highlighted through regular required reporting mechanisms. If grant expenditures exceed the minimum threshold, the five-year inventory management plan will be developed and monitored by FEMA.

Secure Identification

THSGP funds may be used to support the development and production of enhanced tribal documents (e.g., Enhanced Tribal Cards) designed to meet the requirements of the Western Hemisphere Travel Initiative (WHTI). More information on the WHTI may be found at http://www.dhs.gov/files/programs/gc_1200693579776.shtm and <https://www.cbp.gov/travel/us-citizens/western-hemisphere-travel-initiative>.

When completing the IJ Template, please refer to the Goal at for a list of the core capabilities that best fit the proposed activities and costs. For additional assistance in determining the core capabilities that fit the proposed WHTI project, please contact the CSID by phone at (800) 368-6498 or by e-mail at askcsid@fema.gov

Fidelity Bonds

Reasonable costs of fidelity bonds (or like insurance as provided for by applicable state or tribal laws) covering the maximum amount of THSGP funds the officer, official, or employee handles at any given time for all personnel who disburse or approve disbursement of THSGP funds may be allowable if required by the terms and conditions of the award or if generally required by the tribe in its general operations. If a fidelity bond is required by a tribe in its general operations, those costs must be charged as indirect costs. *See* 2 C.F.R. § 200.427.

THSGP 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)(i), 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)(i), Change in Scope Prior Approval, DHS/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 ND Grants 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 period of performance.

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

Program Appendix C: Nonprofit Security Grant Program (NSGP)

NSGP grant recipients and subrecipients 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. Grant funds may not be used for matching funds for other federal grants or cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity.

Pre-award costs are allowable only with the prior written approval of DHS/FEMA and if they are included in the award agreement. To request pre-award costs a written request must be included with the application, signed by the Authorized Organizational Representative of the entity. The letter must outline what the pre-award costs are for, including a detailed budget break-out of pre-award costs from the post-award costs, and a justification for approval. The following information outlines general allowable and unallowable NSGP costs guidance.

NSGP Funding Guidelines

Recipients and subrecipients 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. In administering a NSGP grant award, recipients must comply with the following general requirements:

NSGP Priorities

See the annual NSGP NOFO.

Allowable Costs

Management and Administration (M&A)

M&A activities are those costs defined as directly relating to the management and administration of NSGP funds, such as financial management and monitoring. The amount of M&A is specified in each fiscal year's NSGP NOFO. M&A costs include the following categories of activities:

- Hiring of full-time or part-time staff or contractors/consultants responsible for activities relating to the management and administration of NSGP funds
- Meeting-related expenses directly related to M&A of NSGP funds

Indirect (Facilities and Administrative [F&A]) Costs

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal.

Allowable Direct Costs

Planning

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility and should include consideration of access and functional needs considerations as well as those with limited English proficiency. Examples of planning activities allowable under this program include:

- Development and enhancement of security plans and protocols
- Development or further strengthening of security assessments
- Emergency contingency plans
- Evacuation/Shelter-in-place plans
- Other project planning activities with prior approval from DHS/FEMA

Equipment

Allowable costs are focused on target hardening and physical security enhancements. Funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist attack. This equipment is **limited to select items in the following two sections** of items on the Authorized Equipment List (AEL):

- Physical Security Enhancement Equipment (Section 14)
- Inspection and Screening Systems (Section 15)

The two allowable prevention and protection categories and equipment standards for the NSGP are listed on DHS AEL located on the DHS/FEMA site at <http://www.fema.gov/authorized-equipment-list>. Unless otherwise stated, equipment must meet all mandatory statutory, regulatory, and DHS/FEMA-adopted standards to be eligible for purchase using these funds, including the Americans with Disabilities Act. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 C.F.R. Part 200, including but not limited to 2 C.F.R. §§ 200.310, 200.313, and 200.316.

Exercises

Funding may be used to conduct security-related exercises. This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low-risk setting. All shortcomings or gaps—including those identified for children and individuals with access and functional needs—should be identified in an improvement plan. Improvement plans should be dynamic documents with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. For additional information on HSEEP,

refer to <https://www.fema.gov/exercise>. In accordance with HSEEP guidance, subrecipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. This link provides access to a sample AAR/IP template: <https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning>. Recipients are encouraged to enter their exercise data and AAR/IP in the Preparedness Toolkit at <https://preptoolkit.fema.gov/web/hseep-resources>.

Maintenance and Sustainment

The use of DHS/FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, as described in DHS/FEMA Policy FP 205-402-125-1, *Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants*, located at <http://www.fema.gov/media-library/assets/documents/32474>, under all active and future grant awards, unless otherwise noted.

Grant funds are intended to support the National Preparedness Goal and fund projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in [IB 379: Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#) allows for the expansion of eligible maintenance and sustainment costs that must be in (1) direct support of existing capabilities, (2) must be an otherwise allowable expenditure under the applicable grant program, and (3) be tied to one of the core capabilities in the five mission areas outlined in the Goal. Additionally, eligible costs may also support equipment, training, and critical resources that have previously been purchased with either federal grant or any other source of funding other than DHS/FEMA preparedness grant program dollars.

Construction and Renovation

NSGP funding may not be used for construction and renovation projects without prior written approval from DHS/FEMA. All recipients of NSGP funds must request and receive prior approval from DHS/FEMA before any NSGP funds are used for any construction or renovation. Additionally, recipients are required to submit a SF-424C Budget and budget detail citing the project costs. The total cost of any construction or renovation paid for using NSGP funds may not exceed the greater amount of \$1,000,000.00 or 15% of the NSGP award. Recipients and subrecipients are also 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 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 Program Analyst within six months of the award and completed EHP review materials must be submitted no later than 12 months before the end of the period of performance. EHP review packets should be sent to gpdehpinfo@fema.gov.

NSGP recipients using funds for construction projects must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). 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. Additional information regarding compliance with the *Davis-Bacon Act*, including Department of Labor (DOL) wage determinations, is available from the following website: <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Training

Nonprofit organizations may use NSGP funds for the following training-related costs:

- Employed or volunteer security staff to attend security-related training within the United States;
- Employed or volunteer staff to attend security-related training within the United States with the intent of training other employees or members/congregants upon completing the training (i.e., “train-the-trainer” type courses);
- Nonprofit organization’s employees, or members/congregants to receive on-site security training.

Allowable training-related costs under the NSGP are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and travel expenses are not allowable costs.

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, target hardening, and terrorism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, Active Shooter training, and emergency first aid training. Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization’s IJ. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. ***Proposed attendance at training courses and all associated costs using the NSGP must be included in the nonprofit organization’s IJ.***

Contracted Security Personnel

Contracted security personnel are allowed under this program only as described in the NOFO and Manual and comply with guidance set forth in [IB 421b](#) and [IB 441](#). NSGP funds may not be used to purchase equipment for contracted security. The recipient must be able to sustain this capability in future years without NSGP funding.

Unallowable Costs

The following projects and costs are considered **ineligible** for award consideration:

- Organization costs, and operational overtime costs
- Hiring of public safety personnel
- General-use expenditures
- Overtime and backfill
- Initiatives that do not address the implementation of programs/initiatives to build prevention and protection-focused capabilities directed at identified facilities and/or the surrounding communities
- The development of risk/vulnerability assessment models
- Initiatives that fund risk or vulnerability security assessments or the development of the IJ
- Initiatives in which federal agencies are the beneficiary or that enhance federal property
- Initiatives which study technology development
- Proof-of-concept initiatives
- Initiatives that duplicate capabilities being provided by the Federal Government
- Organizational operating expenses
- Reimbursement of pre-award security expenses

NSGP 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)(i), 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)(i), Change in Scope Notification, DHS/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 ND Grants 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 Investment Justification (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 period of performance.

DHS/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 towards 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.

Furthermore, NSGP project funding is based on the ability of the proposed project to mitigate the risk factors identified in the IJ. For this reason, DHS/FEMA may reject requests to significantly change the physical security enhancements that are purchased with NSGP funding where DHS/FEMA believes approval of the request would change or exceed the scope of the originally approved project. DHS/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)(i).

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

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 100% of funds awarded under NSGP to successful nonprofit applicants 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 Program Analyst. 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 ND Grants system. If an SAA accepts its award within 15 calendar days of receiving notice of the award in the ND Grants 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 ND Grants system, the 45-calendar days pass-through period will begin 15 calendar days after the award notification is sent to the SAA via the ND Grants 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 August 20, 2020, while the POP dates for that award are September 1, 2020, through August 31, 2022. In this example, the 45-day pass-through period will begin on the date the SAA accepts the NSGP award or September 4, 2020 (15 calendar days after the SAA was notified of the award), whichever date occurs first. The POP start date of September 1, 2020 would not affect the timing of meeting the 45-calendar day pass-through requirement.

DUNS/SAM Requirements for Recipients and Subrecipients

As the direct applicant and recipient of NSGP funding, the SAA is required to have a DUNS number and be registered in SAM and must maintain the currency of the SAA's information in SAM until the SAA submits the final financial report required under the award or receives final payment, whichever is later. Nonprofit organizations that are first-tier subrecipients applying for NSGP funding through the SAA must have a DUNS number, but are not required to be registered in SAM.

Program Appendix D: Transit Security Grant Program (TSGP)

TSGP grant recipients may only use TSGP grant funds for the purpose set forth in the NOFO, and all investments must be consistent with the statutory authority for the award. Grant funds may not be used for matching funds for other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity.

Applicable Regulations

Costs charged to a TSGP 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. For more information on 2 C.F.R. Part 200, please see IB 400 regarding FEMA's implementation of these provisions, available at https://www.fema.gov/media-library-data/1419366341862-296dd0cc30bbf64a6b45581afe9d8b17/InformationBulletin400_2CFERPart200_FINAL.pdf.

Pre-Award Costs

Pre-award costs are not allowable and will not be approved, with the exception of costs resulting from pre-award grant writing services provided by an independent contractor that shall not exceed \$1,500.00. See below for more information on these costs.

TSGP Priorities

See the annual TSGP NOFO.

Allowable Direct Costs

Specific investments made in support of the funding priorities in the annual TSGP NOFO generally fall into one of the following six allowable expense categories:

- Planning
- Operational Activities
- Equipment and Capital Projects
- Training and Awareness Campaigns
- Exercises
- Management and Administration

The following provides guidance on allowable costs within each of these areas:

Planning

Planning activities address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Planning Priorities.

TSGP funds may be used for the following types of planning activities:

- Development and enhancement of system-wide security risk management plans, to include cyber
- Development or further strengthening of continuity of operations plans, response plans, station action plans, risk assessments, and asset-specific remediation plans
- Development or further strengthening of security assessments, including multi-agency and multi-jurisdictional partnerships and conferences to facilitate planning activities
- Hiring of full or part-time staff and contractors or consultants to assist with planning activities only to the extent that such expenses are for the allowable activities within the scope of the grant (not for the purpose of hiring public safety personnel)
- Materials required to conduct planning activities
- Other project planning activities with prior approval from DHS/FEMA

Operational Activities

Operational Activities address the Soft Targets/Crowded Places; and Emergent Threat Priorities.

DHS/FEMA encourages applicants to develop innovative operational approaches to enhance the security of transit systems. Projects that use visible, unpredictable deterrence, to include operational packages dealing with explosive detection canine teams, mobile screening teams, and anti-terrorism teams, directly support enhancing the protection of soft targets and crowded places. Implementation of one of the three Operational Package (OPack) models discussed below complements existing security systems and provides an appropriate, practical, and cost-effective means of protecting assets.

Agencies may submit IJs to fund transit security police forces/law enforcement providers for patrols and activities on overtime, such as directed patrols, additional canine teams, mobile screening teams, or anti-terrorism team patrols. These activities must be dedicated to the transit environment and must be anti-terrorism in nature. Agencies must identify the type of activity, length of operation (hours), number of personnel, and cost based on length of operation and personnel. Agencies should also provide a risk-based justification for the request, to include linkage to a known event, such as hosting a significant regional sporting or political event; or a period of heightened awareness, such as a national holiday. Three OPack types have been developed to support operational activities and are available for funding under the TSGP:

- **Explosives Detection Canine Teams (EDCTs).** When combined with the existing capability of a transit security/police force, the added value provided through the addition of an EDCT is significant. EDCTs are a proven, reliable resource to detect explosives and are a key component in a balanced counter-sabotage program. The TSGP will provide funds to establish dedicated security/police force canine teams. Each canine team will be composed of one dog and one handler.
- **Anti-Terrorism Teams (ATTs).** The ATT capability provided through TSGP funding is for uniformed, dedicated transit patrols on a normal operational basis, rather than using teams only for a surge capacity as provided by DHS/FEMA in the past. ATTs do not supersede other local transit security forces; rather, they augment current capabilities. Each ATT will consist of four individuals, including two overt elements (*e.g.*, uniformed transit sector law enforcement officer, canine team, mobile explosive screeners), and two discreet observer elements.
- **Mobile Explosive Screening Teams (MESTs).** The MEST OPack will allow recipients the flexibility to deploy combinations of trained individuals and technologies that will assist in making screening decisions where there are large numbers of individuals with hand carried items. This screening technology will be coupled with mobile explosive screening technologies.

Note: Funds for canine teams may not be used to fund drug detection and apprehension technique training. Only explosives detection training for the canine teams will be funded.

Five-Year Security Capital Plan and Operational Sustainment

Applicant requests for OPack funding must include the submission of a Five-Year Security Capital and Operational Sustainment Plan in ND Grants. This plan must include how the agency proposes to implement capital projects and demonstrate how the agency will sustain the operational investments (including officers hired with federal funding) and capabilities after grant funding has been expended. ***Requests for OPacks will not be funded if the applicant does not have a Security Capital and Operational Sustainment Plan.***

Funding Availability for OPacks

OPacks have the potential to be funded for up to a 36-month period from the award date. The monetary figures presented below are stated in terms of cost per period of performance (which indicates actual/complete funding for the 36-month period). Additionally, any OPack costs after the 36-month period of performance (including expenses related to the maintenance, personnel, equipment, etc.) are the responsibility of the applicable transit system. Additional funding may be applied for in future grant cycles to maintain this operational capability, but future funding is not guaranteed and requires approval. If these positions are not sustained, the public transportation agency may not be eligible for this personnel support in the future. The table below identifies the maximum funding available for the different OPack types.

Available Funding for OPacks

Operational Package	Maximum Funding per Year (12 months)	Maximum Funding per Period of Performance (36 months)
EDCT	\$150,000 per team	\$450,000 per team
ATT	\$500,000 per team	\$1,500,000 per team
MEST	\$600,000 per team	\$1,800,000 per team

OPack Requirements

TSGP OPack funds may be used for new positions or to sustain existing capabilities/programs (e.g., canine teams) already supported by the recipient. Applicants pursuing both new OPacks and sustainment funding for existing OPacks must indicate in their IJs which funding the higher priority for their agency is. Additionally, applicants must provide the number of existing teams (EDCT, ATT, and MEST) already in place with either in-house funding or TSGP funding. The table below identifies specific OPack requirements.

OPack Requirements

Operational Package	Requirements
Explosives Detection Canine Teams	Please refer to the pages below for detailed information regarding EDCTs under the TSGP

Operational Package	Requirements
Anti-Terrorism Teams	<p>Specific for the Canine Team within the ATT:</p> <ul style="list-style-type: none"> • Each canine team, composed of one dog and one handler, must be certified by an appropriate, qualified organization • Canines should receive an initial basic training course and also weekly maintenance training sessions thereafter to maintain the certification • The basic training averages 10 weeks for the team, 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 United States Police Canine Association (USPCA), or the International Explosive Detection Dog Association (IEDDA) may be used to meet this requirement • The individuals hired for the covert and overt elements must be properly trained law enforcement officers • Certifications should be on file with the recipient and must be made available to DHS/FEMA upon request
Mobile Explosives Screening Team	Certifications should be on file with the recipient and must be made available to DHS/FEMA upon request

Allowable Expenses for OPacks

The below table identifies allowable expenses for the various OPacks. Please see the inserted notes for clarification of certain allowable costs.

Allowable Expenses for OPacks

Operational Package		Salary and Fringe Benefits	Training and Certification	Equipment Costs	Purchase and Train a Canine	Canine Costs ^b
1)	EDCT	✓	✓	✓	✓ ^c	✓
2)	ATT	✓	✓	✓	✓	✓
3)	Mobile Explosives Screening Team	✓		✓ ^d		
<p>a Travel costs associated with training for personnel, handlers, and canines are allowable</p> <p>b Canine costs include but are not limited to: veterinary, housing, and feeding costs</p> <p>c One type of allowable training is training specific to the detection of common explosives odors.</p> <p>d Equipment and other costs can include but are not limited to explosives detection; stainless steel search tables; consumables such as gloves, swabs, and alcohol; and land mobile radios</p>						

Specific Guidance on Explosive Detection Canine Teams (EDCT)

EDCT Certification. Each 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 (i.e. TSGP-grant supported) will maintain certification, utilization, and training data to show their compliance in meeting or exceeding those guidelines set forth by the Scientific Working Group on Dog and Orthogonal Detection Guidelines (SWGDOG), as of September 14, 2007, in addition to requirements set forth in the NOFO.

EDCT 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 DHS/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, seven days per week on an on-duty or off-duty on call basis. If TSGP-funded EDCTs are not available, other non-TSGP-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) Recipient EDCTs 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, terminal/platform, luggage, freight/warehouse, 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 DHS/FEMA upon request.
- 6) The TSGP grant 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. Recipient EDCTs will also ensure that such activities include, over a period of time, 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) Recipient EDCTs 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 the 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.
- 8) Recipient EDCTs will ensure that adequate routine and emergency veterinary care are provided for all canines.

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

Equipment and Capital Projects

Equipment and Capital Projects address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Equipment/Capital Projects Priorities.

Priority projects include Top Transit Asset List risk remediation and protection of other high-risk, high-consequence areas or systems that have been identified through system-wide risk assessments.

- Projects related to physical security enhancements at rail and bus stations in UASI jurisdictions including security cameras, security screening equipment for people and baggage, and access control (e.g. fences, gates, barriers, etc.).
- Projects related to cybersecurity of access control, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls, etc. or passenger/vehicle/cargo security screening equipment support. Cybersecurity assessments are allowable.

Equipment Acquisition

TSGP funds must comply with [IB 426: Guidance to Recipients and Subrecipients of FEMA Preparedness Grants Regarding Implementation of Executive Order 13809 Restoring State, Tribal, Territorial, and Local Law Enforcement's Access to Life-Saving Equipment and Resources](#). TSGP funds may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found in the [DHS Authorized Equipment List \(AEL\)](#). These costs include:

- Personal protection equipment
- Explosive device mitigation and remediation equipment
- Chemical, biological, radiological, nuclear, and high explosive (CBRNE) operational search and rescue equipment, logistical support equipment, reference materials, or incident response vehicles
- Interoperable communications equipment
- Components or systems needed to address flaws in the computerized systems that control generators, switching stations, and electrical substations as well as other emerging threats to infrastructure critical to the U.S. economy
- Detection Equipment
- Power equipment
- Terrorism incident prevention equipment
- Physical security enhancement equipment

Unless otherwise noted, equipment must be certified as meeting required regulatory and DHS/FEMA-adopted standards to be eligible for purchase using TSGP funds. Equipment must comply with the *Occupational Safety and Health Act* requirement for certification of electrical equipment by a nationally recognized testing laboratory and demonstrate compliance with relevant DHS/FEMA-adopted standards through a supplier's declaration of conformity with appropriate supporting data and documentation per International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17050, Parts One and Two. Agencies must have all necessary certifications and licenses for the requested equipment, as appropriate, prior its purchase. DHS adopted standards are found at:

<https://www.dhs.gov/dhs-implementation-statement-regarding-standard-terms-and-conditions-research-grants>. In addition, recipients that are using TSGP funds to support emergency communications equipment activities must comply with the *SAFECOM Guidance for Emergency Communication Grants*, including provisions on technical standards that ensure and enhance interoperable communications. This *SAFECOM* Guidance can be found at <https://www.dhs.gov/safecom>.

Equipment: Requirements for Small Unmanned Aircraft Systems

All requests to purchase Small Unmanned Aircraft Systems (SUAS) with DHS/FEMA grant funding must comply with [IB 426](#) and must include a description of the policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties of the jurisdiction that will purchase, take title to, or otherwise use the SUAS equipment.

Cybersecurity Projects

TSGP funds may be used for projects that enhance the cybersecurity of:

- Access controls, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls (such as firewalls, network segmentation, predictive security cloud, etc.)
- Passenger/vehicle/cargo security screening equipment (cybersecurity assessments are allowable)

When requesting funds for cybersecurity, applicants are encouraged to propose projects that would aid in implementation of all or part of the [Framework for Improving Critical Infrastructure Cybersecurity](#) (the "Framework") developed by the National Institute of Standards and Technology (NIST). The Framework gathers existing international standards and practices to help organizations understand, communicate, and manage their cyber risks. For organizations that do not know where to start with developing a cybersecurity program, the Framework provides initial guidance. For organizations with more advanced practices, the Framework offers a way to improve their programs, such as better communication with their leadership and suppliers about management of cyber risks.

DHS's Critical Infrastructure Cyber Community C³ Voluntary Program also provides resources to critical infrastructure owners and operators to assist in adoption of the Framework and managing cyber risks. Additional information on the Critical Infrastructure Cyber Community C³ Voluntary Program can be found at www.dhs.gov/ccubedvp.

DHS's Enhanced Cybersecurity Services (ECS) program is an example of a resource that assists in protecting U.S.-based public and private entities and combines key elements of capabilities under the "Detect" and "Protect" functions to deliver an impactful solution relative to the outcomes of the Cybersecurity Framework. Specifically, ECS offers intrusion prevention and analysis services that help U.S.-based companies and SLTT governments defend their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sourcing timely, actionable cyber threat indicators from sensitive and classified Government Furnished Information (GFI). DHS then shares those indicators with accredited Commercial Service Providers (CSPs). Those CSPs in turn use the indicators to block certain types of malicious traffic from entering a company's networks. Groups interested in subscribing to ECS must contract directly with a CSP in order to receive services. Please visit <http://www.dhs.gov/enhanced-cybersecurity-services> for a current list of ECS CSP points of contact.

Capital (Construction) Projects Guidance

Recipients must obtain written approval from FEMA prior to the use of any TSGP funds for construction or renovation projects. When applying for construction funds, including communications towers, at the time of application, recipients must submit evidence of approved zoning ordinances, architectural plans, and any other locally required planning permits. Additionally, recipients are required to submit a SF-424C and budget detail citing the project costs.

Recipients are also 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 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](#), instances must also be identified to the FEMA HQ Program Analyst within the first six months of the award, regardless of the period of performance. Completed EHP review materials for construction and communication tower projects must be submitted no later than 12 months before the end of the period of performance. EHP Technical Assistance, including the EHP Screening Form, can be found online at: <https://www.fema.gov/media-library/assets/documents/90195>. EHP review materials should be sent to gpdehpinfo@fema.gov.

TSGP recipients using funds for construction projects must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). 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. Additional information regarding compliance with the *Davis-Bacon Act*, including Department of Labor (DOL) wage determinations, is available at <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Training and Awareness Campaigns

Training and Awareness Campaigns address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Training and Awareness Campaign Priorities.

Training

TSGP funds may be used for the following training activities:

- **Training Topics.** Priority topics include active shooter training, security training for employees, and public awareness/preparedness campaigns.
- **Training Workshops.** Grant funds may be used to plan and conduct training workshops to include costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel, and training plan development. Recipients are strongly encouraged to use free public space/locations/facilities, whenever available, prior to the rental of space/locations/facilities. Training should provide the opportunity to demonstrate and validate skills learned, as well as to identify any gaps in these skills. Any training or training gaps, including those for children and individuals with disabilities or access and functional needs, should be identified in an After-Action Report/Improvement Plan (AAR/IP) and addressed in the training cycle.
- **Hiring of Full or Part-Time Staff or Contractors/Consultants.** Full or part-time staff or contractors/consultants may be hired to support training-related activities. Reimbursement of these costs should conform with the policies of the state or local unit(s) of government or the awarding agency, whichever is applicable. Such costs must be included within the funding allowed for program management personnel expenses, which must not exceed 10% of the total allocation. Dual compensation is unallowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government and from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both activities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.
- **Overtime and Backfill Costs.** The entire amount of overtime costs, including payments related to backfilling personnel, that are the direct result of attendance at FEMA and approved training courses and programs are allowable. Reimbursement of these costs should follow the policies of

the state or local unit(s) of government or the awarding agency, whichever is applicable. In no case is dual compensation allowable.

- **Travel.** Domestic travel costs (e.g., airfare, mileage, per diem, and hotel) are allowable as expenses by employees who are on travel status for official business related, approved training, subject to the restrictions at 2 C.F.R. Part 200. International travel is not an allowable expense.
- **Supplies.** Supplies, items that are expended or consumed during the course of the planning and conduct of the training project(s) (e.g., gloves and non-sterile masks), are allowable expenses.
- **Funds Used to Develop, Deliver, and Evaluate Training,** including costs related to administering the training, planning, scheduling, facilities, materials and supplies, reproduction of materials, and equipment are allowable expenses. Training should provide the opportunity to demonstrate and validate skills learned, as well as to identify any gaps in these skills. Any training or training gaps, including those for children and individuals with disabilities or access and functional needs, should be identified in the AAR/IP and addressed in the training cycle.

Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model of instruction design. Information on DHS/FEMA-approved training can be found at <http://www.firstrespondertraining.gov/>.

Awareness Campaigns

TSGP funds may be used for the development and implementation of awareness campaigns to raise public awareness of indicators of terrorism and terrorism-related crime, and for associated efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. DHS currently sponsors or supports a number of awareness campaigns. Please review materials, strategies and resources at <https://www.dhs.gov/dhs-campaigns> before embarking on the development of an awareness campaign for local constituencies and stakeholders.

Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS “If You See Something, Say Something®” campaign using grant funds work directly with the DHS Office of Partnership and Engagement (OPE). This will help ensure that the awareness materials (e.g., videos, posters, tri-folds, etc.) remain consistent with DHS’s messaging and strategy for the campaign and compliant with the initiative’s trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the Campaign’s Office (seesay@hq.dhs.gov), must be facilitated by the FEMA HQ Program Analyst.

Exercises

Exercise activities address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Exercises Priorities.

TSGP funds may be used for the following exercise activities:

- **Funds Used to Design, Develop, Conduct and Evaluate an Exercise.** This includes costs related to planning, meeting space, and other meeting costs, facilitation costs, materials and supplies, travel, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low-risk setting. Any shortcoming or gap identified, including those for children and individuals with disabilities or access and functional needs, should be identified in an effective corrective action program that includes development of improvement plans that are dynamic documents, with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

- **Hiring of Full or Part-Time Staff or Contractors/Consultants.** Full or part-time staff may be hired to support exercise-related activities. In order to be eligible for reimbursement, the costs for hiring staff must conform to the policies of the non-Federal entity and Federal statutes, where applicable. *See, e.g.,* 2 C.F.R. § 200.430(a). The costs for hiring contractors or consultants must comply with the applicable Federal procurement standards at 2 C.F.R. §§ 200.317 – 200.326. The costs for hiring staff, consultants, or contractors to support exercise-related activities costs must be included within the funding allowed for program management personnel expenses, which must not exceed 10% of the total allocation. Dual compensation is never allowable, meaning, in other words, that an employee of a unit of government may not receive compensation from their unit or agency of government and from an award for a single period of time (*e.g.,* 1:00 p.m. to 5:00 p.m.), even though their work may benefit both entities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.
- **Overtime and Backfill Costs.** The entire amount of overtime costs, including payments related to backfilling personnel, which are the direct result of time spent on the design, development and conduct of exercises are allowable expenses. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or the awarding agency, whichever is applicable. Dual compensation is never allowable.
- **Travel.** Domestic travel costs are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of exercise project(s), subject to the restrictions at 2 C.F.R. Part 200. International travel is not an allowable expense.
- **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (*e.g.,* gloves, non-sterile masks, and disposable protective equipment).
- **Other Items.** These costs include the rental of space/locations for exercise planning and executing, rental of equipment, etc. Recipients are encouraged to use free public space/locations/facilities, whenever available, prior to the rental of space/locations/facilities. These also include costs that may be associated with inclusive practices and the provision of reasonable accommodations and modifications to provide full access for children and adults with disabilities.

Management and Administration (M&A)

Management and administration costs are allowed under this program. M&A costs are activities directly related to managing and administering the award. Recipients may use up to 5% of the amount of the award for their M&A.

Current fiscal year TSGP funds may be used for the following M&A costs:

- Hiring of full-time or part-time staff, including contractors and consultants, to execute the following:
 - Management of the current fiscal year TSGP Award
 - Design and implementation of the current fiscal year TSGP submission meeting compliance with reporting/data collection requirements, including data calls
 - Information collection and processing necessary to respond to DHS/FEMA data calls
 - Domestic-only travel expenses related to TSGP grant administration, in compliance with 2 C.F.R. Part 200.
 - Acquisition of authorized office equipment, including personal computers or laptops for TSGP M&A purposes

Allowable Indirect Costs

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal.

Unallowable Costs

Specific unallowable costs include:

- ***Grant funds must comply with [IB 426](#) and may not be used for the purchase of the following equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.*** Additional prohibited equipment expenditures include items unrelated to grant allowable activities, such as general-use software, general-use computers and related equipment (other than for allowable M&A activities or otherwise associated preparedness or response functions), general-use vehicles, and licensing fees.
- Personnel costs (except as detailed above).
- Activities unrelated to the completion and implementation of the TSGP.
- Other items not in accordance with the AEL or not previously listed as allowable costs.

Maintenance and Sustainment Costs

The use of FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, as described in FEMA Policy FP 205- 402-125-1 (located at <http://www.fema.gov/media-library/assets/documents/32474>), under all active and future grant awards, unless otherwise noted.

Grant funds are intended to support the National Preparedness Goal and fund projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in [IB 379: Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#) allows for the expansion of eligible maintenance and sustainment costs that must be in (1) direct support of existing capabilities; (2) must be an otherwise allowable expenditure under the applicable grant program, and (3) be tied to one of the core capabilities in the five mission areas outlined in the Goal. Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant or any other source of funding other than DHS/FEMA preparedness grant program dollars.

Encouraged Use of Certain Products Produced in the United States

Pursuant to Executive Order 13858 “[Strengthening Buy-American Preferences for Infrastructure Projects](#),” FEMA encourages non-federal entities under this grant program to use, to the greatest extent practicable and consistent with the law, iron and aluminum as well as steel, cement, and other manufactured products produced in the United States, in projects funded by an award under this grant program affecting surface transportation, including roadways, bridges, railroads, and transit; aviation;

ports, including navigational channels; water resources projects; energy production, generation, and storage, including from fossil-fuels, renewable, nuclear, and hydroelectric sources; electricity transmission; gas, oil, and propane storage and transmission; electric, oil, natural gas, and propane distribution systems; broadband internet; pipelines; stormwater and sewer infrastructure; drinking water infrastructure; and cybersecurity.

Notwithstanding this encouragement, non-federal entities must take care that all procurements and contract actions are consistent with law, the Preparedness Grants Manual and applicable appendices, the grant program's NOFO, and the Federal procurement standards at 2 C.F.R. §§ 200.317-200.326.

Program Appendix E: Intercity Bus Security Grant Program (IBSGP)

IBSGP grant recipients may only use IBSGP grant funds for the purpose set forth in the NOFO, and all investments must be consistent with the statutory authority for the award. Grant funds may not be used for matching funds for other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity.

Applicable Regulations

Costs charged to an 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. For more information on 2 C.F.R. Part 200, please visit https://www.fema.gov/media-library-data/1419366341862-296dd0cc30bbf64a6b45581afe9d8b17/InformationBulletin400_2CFRPart200_FINAL.pdf.

IBSGP Priorities

See the annual IBSGP NOFO.

Pre-Award Costs

Pre-award costs are not allowable and will not be approved, with the exception of costs resulting from pre-award grant writing services provided by an independent contractor that shall not exceed \$1,500. See the IBSGP NOFO for more information.

Allowable Direct Costs

Specific investments made in support of the funding priorities discussed in the annual IBSGP NOFO generally fall into one of the following six allowable expense categories:

1. Planning
2. Operational Activities
3. Equipment and Capital Projects
4. Training and Awareness Campaigns
5. Exercises
6. Management and Administration

The following provides guidance on allowable costs within each of these areas.

Planning

Planning activities should address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Planning Priorities.

IBSGP funds may be used for the following types of planning activities:

- Development and enhancement of system-wide security risk management plans, to include cyber

- Development or further strengthening of continuity of operations plans, response plans, station action plans, risk assessments, and asset-specific remediation plans
- Development or further strengthening of security assessments, including multi-agency and multi-jurisdictional partnerships and conferences to facilitate planning activities
- Hiring of full- or part-time staff and contractors or consultants to assist with planning activities only to the extent that such expenses are for the allowable activities within the scope of the grant (not for the purpose of hiring public safety personnel)
- Materials required to conduct planning activities
- Other project planning activities with prior approval from DHS/FEMA

Operational Activities

Operational Activities should address the Soft Targets/Crowded Places; and Emergent Threat Priorities.

DHS/FEMA encourages applicants to develop innovative operational approaches to enhance the security of transit systems. Examples include:

- Establishing or improving emergency communication systems linking drivers and over-the-road buses to company operation centers, law enforcement agencies or emergency response personnel
- Acquiring and installing equipment or systems that collect, store or exchange passenger and/or driver information with established government databases for security purposes
- Implementing and operating established methodologies for screening passengers, their carry-on baggage, and/or their checked baggage, for weapons and/or explosives

Equipment and Capital Projects

Equipment and Capital Projects should address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Equipment/Capital Projects Priorities.

Equipment – Vehicle/Driver Security Enhancements

Vehicle Security Enhancements focus on vehicle disabling and anti-theft devices, real-time bus inventory and inventory control, tracking, monitoring, and locating technologies. Driver security enhancements focus on protection for the bus driver to prevent would-be terrorists from immobilizing the driver and/or hijacking the bus. Applicants are discouraged from submitting projects that propose the use of closed-circuit television (CCTV) alone as an on-board deterrent to terrorism. Rather, any cameras should have the capability and protocols in place for incident-based real-time monitoring. CCTV Systems that are primarily archival, and do not clearly specify the ability for live monitoring in the IJ will not be funded.

Capital Projects – Facility Security Enhancements

- Projects related to physical security enhancements at bus stations, or operator-owned facilities including but not limited to lighting, security cameras, security screening equipment for people and baggage, and access control (e.g. fences, gates, barriers).
- Projects related to cybersecurity of access control, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls, etc. or passenger/vehicle/cargo security screening equipment support. Cybersecurity assessments are allowable.
- Full or Part-Time Staff or Contractors/Consultants. Full or part-time staff or contractors/consultants may be hired to support security enhancement-related activities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.

Note: All Capital and Vehicle/Driver security enhancement projects that include cameras, video surveillance, or alarm systems MUST either be live monitored 24/7 or have the capability for real-time

incident-based monitoring. CCTV Systems that are primarily archival and do not clearly specify the ability for live monitoring in the IJ will not be funded.

Equipment Acquisition

IBSGP funds must comply with [IB 426](#) and may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found in the [DHS Authorized Equipment List \(AEL\)](#). These costs include:

- Personal protection equipment
- Explosive device mitigation and remediation equipment
- Chemical, biological, radiological, nuclear, and high explosive (CBRNE) operational search and rescue equipment, or logistical support equipment
- Interoperable emergency communications equipment
- Detection equipment
- Terrorism incident prevention equipment
- Physical security enhancement equipment

Unless otherwise noted, equipment must be certified as meeting required regulatory and DHS- adopted standards to be eligible for purchase using these funds. Equipment must comply with the *Occupational Safety and Health Act* requirement for certification of electrical equipment by a nationally recognized testing laboratory and demonstrate compliance with relevant DHS-adopted standards through a supplier's declaration of conformity with appropriate supporting data and documentation per International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17050, Parts One and Two. Agencies must have all necessary certifications and licenses for the requested equipment, as appropriate, prior to the request. In addition, recipients that are using IBSGP funds to support emergency communications equipment activities must comply with the *SAFECOM Guidance for Emergency Communication Grants*, including provisions on technical standards that ensure and enhance interoperable communications. *SAFECOM Guidance* can be found at: <https://www.dhs.gov/safecom>.

Cybersecurity Projects

IBSGP funds may be used for projects that enhance the cybersecurity of:

- Access controls; sensors; security cameras; badge/ID readers; Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) systems; process monitors and controls (such as firewalls, network segmentation, predictive security cloud, etc.). CCTV Systems that are primarily archival, and do not clearly specify the ability for live monitoring in the IJ will not be funded.
- Passenger/vehicle/cargo security screening equipment (cybersecurity assessments are allowable).

When requesting funds for cybersecurity, applicants are encouraged to propose projects that would aid in implementation of all or part of the [Framework for Improving Critical Infrastructure Cybersecurity](#) (“The Framework”) developed by the National Institute of Standards and Technology (NIST). The Framework gathers existing international standards and practices to help organizations understand, communicate, and manage their cyber risks. For organizations that do not know where to start with developing a cybersecurity program, the Framework provides initial guidance. For organizations with more advanced practices, the Framework offers a way to improve their programs, such as better communication with their leadership and suppliers about management of cyber risks.

DHS's Critical Infrastructure Cyber Community C³ Voluntary Program also provides resources to critical infrastructure owners and operators to assist in adoption of the Framework and managing cyber risks. Additional information on the Critical Infrastructure Cyber Community C³ Voluntary Program can be found at www.dhs.gov/ccubedvp.

DHS's Enhanced Cybersecurity Services (ECS) program is an example of a resource that assists in protecting U.S.-based public and private entities and combines key elements of capabilities under the "Detect" and "Protect" functions to deliver an impactful solution relative to the outcomes of the Cybersecurity Framework. Specifically, ECS offers intrusion prevention and analysis services that help U.S.-based companies and SLTT governments defend their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sourcing timely, actionable cyber threat indicators from sensitive and classified Government Furnished Information (GFI). DHS then shares those indicators with accredited Commercial Service Providers (CSPs). Those CSPs in turn use the indicators to block certain types of malicious traffic from entering a company's networks. Groups interested in subscribing to ECS must contract directly with a CSP in order to receive services. Please visit <http://www.dhs.gov/enhanced-cybersecurity-services> for a current list of ECS CSP points of contact.

Capital (Construction) Projects Guidance

Recipients must obtain written approval from FEMA prior to the use of any IBSGP funds for construction or renovation projects. When applying for construction funds, including communications towers, at the time of application, recipients must submit evidence of approved zoning ordinances, architectural plans, any other locally required planning permits. Additionally, recipients are required to submit a SF-424C and budget detail citing the project costs.

Recipients are also 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 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](#), instances must also be identified to the FEMA HQ Program Analyst within the first six months of the award. Completed EHP review materials for construction and communication tower projects must be submitted no later than 12 months before the end of the period of performance. EHP Technical Assistance, including the EHP Screening Form, can be found online at: <https://www.fema.gov/media-library/assets/documents/90195>. EHP review materials should be sent to gpdehpinfo@fema.gov.

IBSGP recipients using funds for construction projects must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). Grant recipients must ensure that their contractors or sub-contractors 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 following website at <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Training and Awareness Campaigns

Training and Awareness Campaigns address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Training and Awareness Campaign Priorities.

Training

IBSGP funds may be used for the following training activities:

- **Training Topics.** Priority topics include active shooter training, security training for employees, and public awareness/preparedness campaigns. Your Investment Justification Narrative for Training should include:
 - A course syllabus, curriculum, or topic plan identifying the proposed course material and contents
 - Provide the total cost of the training course, the number of participants, and the cost per participant breakdown
- **Training Workshops.** Grant funds may be used to plan and conduct training workshops or conferences including costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel, and training plan development.
- **Hiring of Full or Part-Time Staff or Contractors/Consultants.** Full or part-time staff may be hired to support training-related activities. The services of contractors/consultants may also be procured in the design, development, conduct, and evaluation of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) training. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.
- **Overtime and Backfill Costs.** Overtime and backfill costs associated with the design, development, and conduct of training are allowable expenses. Payment of overtime expenses will be for work performed by recipient or subrecipient employees in excess of the established work week related to the planning and conduct of the training project(s). Furthermore, overtime payments and backfill costs associated with sending personnel to training are allowable. Grant funds cannot be used for personnel or direct salary costs for employees to attend training sessions. Recipients seeking to claim overtime or backfill costs will be required to submit verification. Straight time costs are not eligible expenses.
- **Travel.** Domestic travel costs (e.g., airfare, mileage, per diem, hotel, etc.) are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of the training project(s) or for attending courses. These costs must be in accordance with applicable State law and regulations as well as the principles at 2 C.F.R. Part 200. International travel is not an allowable cost under IBSGP
- **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the training project(s) (e.g., copying paper, gloves, tape, and non-sterile masks).
- **Funds Used to Develop, Deliver, and Evaluate Training,** including costs related to administering the training, planning, scheduling, facilities, materials and supplies, reproduction of materials, and equipment are allowable expenses. Training should provide the opportunity to demonstrate and validate skills learned, as well as to identify any gaps in these skills. Any training or training gaps, including those for individuals with disabilities or access and functional needs, should be identified in the AAR/IP and addressed in the training cycle.
- Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model of instructional design. Information on DHS/FEMA-approved training can found at the following website
- **Other Items.** These costs include the rental of space/locations for planning and conducting training, badges, etc. Recipients are encouraged to use free public space/locations, whenever available, prior to the rental of space/locations.

Awareness Campaigns

IBSGP funds may be used for the development and implementation of awareness campaigns to raise public awareness of indicators of terrorism and terrorism-related crime, and associated efforts to increase

the sharing of information with public and private sector partners, including nonprofit organizations. DHS currently sponsors or supports a number of awareness campaigns. Please review materials, strategies and resources at <https://www.dhs.gov/dhs-campaigns> before embarking on the development of an awareness campaign for your local constituencies and stakeholders.

Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS “If You See Something, Say Something®” campaign using grant funds work directly with the DHS Office of Partnership and Engagement (OPE). This will help ensure that the awareness materials (e.g., videos, posters, tri-folds, etc.) remain consistent with the Department’s messaging and strategy for the campaign and compliant with the initiative's trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the Campaign’s Office (seesay@hq.dhs.gov), must be facilitated by the FEMA HQ Program Analyst.

Exercises

Exercise activities should address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Exercises Priorities.

IBSGP funds may be used for the following exercise activities:

- **Funds Used to Design, Develop, Conduct, and Evaluate an Exercise.** This includes costs related to planning, meeting space, and other meeting costs, facilitation costs, materials and supplies, travel, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low-risk setting. Any shortcoming or gap identified, including those for children and individuals with disabilities or access and functional needs, should be identified in an effective corrective action program that includes development of improvement plans that are dynamic documents, with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.
- **Hiring of Full or Part-Time Staff or Contractors/Consultants.** Full or part-time staff may be hired to support exercise-related activities. The services of contractors/consultants staff may be procured to support exercise-related activities. The services of contractors/consultants may also be procured to support the design, development, conduct, and evaluation of terrorism exercises.
- **Overtime and Backfill Costs.** Overtime and backfill costs associated with the design, development, and conduct of terrorism exercises are allowable expenses. Payment of overtime expenses will be for work performed in excess of the established work week related to the planning and conduct of the exercise project(s). Further, overtime payments and backfill costs associated with sending personnel to exercises are allowable, provided that the event being attended is a DHS sponsored exercise. For positions not funded by the grant award, grant funds cannot be used for personnel or straight salary costs for employees to attend exercises, meaning straight time costs for non-grant funded employees to attend exercise are not allowable. Instead, for positions not funded by the grant award, only overtime and backfill costs will be allowable for those employees to attend exercises. Recipients seeking to claim overtime or backfill costs will be required to submit verification.
- **Travel.** Domestic travel costs (e.g., airfare, mileage, per diem, hotel, etc.) are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of the exercise project(s). International travel is not allowable under this program.
- **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (e.g., gloves, non-sterile masks, and disposable protective equipment).

- **Other Items.** These costs include the rental of space/locations for exercise planning and executing, rental of equipment, etc. Recipients are encouraged to use free public space/locations/facilities, whenever available, prior to the rental of space/locations/facilities. These also include costs that may be associated with inclusive practices and the provision of reasonable accommodations and modifications to provide full access for children and adults with disabilities.

Management and Administration (M&A)

Management and administration costs are allowed under this program. M&A costs are activities directly related to managing and administering the award. Recipients may use up to 5% of the amount of the award for their M&A.

Current fiscal year IBSGP funds may be used for the following M&A costs:

- Hiring of full-time or part-time staff including contractors and consultants, to execute the following:
 - Management of the current fiscal year IBSGP Award
 - Design and implementation of the current fiscal year IBSGP submission meeting compliance with reporting/data collection requirements, including data calls
- Information collection and processing necessary to respond to DHS/FEMA data calls
- Domestic travel expenses related to IBSGP grant administration

Indirect Costs (Facilities and Administration [F&A])

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal.

Unallowable Costs

Specific unallowable costs include:

- Grant funds must comply with [IB 426](#) and may not be used for the purchase of the following equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.
- General-use facility expenditures, to include, but not limited to ordinary facility maintenance, contracts for maintenance, and specifically backup or emergency generators
- General vehicle maintenance, service contracts, or warranties. This is different from maintenance and sustainment costs that are allowable, but only for projects funded under a grant award. For projects or equipment not funded by the grant award, general maintenance, service contracts, and warranties are not allowable.
- Expenditures for items such as general-use software (word processing, spreadsheet, graphics, etc.), general-use computers and related equipment (other than for allowable M&A activities, or otherwise associated preparedness or response functions), general-use vehicles, licensing fees, recurring operating costs (e.g., cell phone services, maintenance contracts).
- Organizational operating expenses
- Personnel costs, to include, but not limited to, overtime and backfill (except as detailed above).

- Activities unrelated to the completion and implementation of the IBSGP.
- Other indirect costs (meaning property purchase, depreciation, or amortization expenses)
- Initiatives in which federal agencies are the beneficiary or that enhance federal property
- Initiatives which study technology development
- Proof-of-concept initiatives
- Initiatives that duplicate capabilities being provided by the Federal government
- Other items not in accordance with the Authorized Equipment List (AEL), in accordance with IB 426, or not previously listed as allowable costs.
- Pre-award costs are not allowable and will not be approved, with the exception of costs resulting from pre-award grant writing services provided by an independent contractor that shall not exceed \$1,500, as detailed in “Pre-Award Costs” above and in the IBSGP NOFO.

Other Allowable Costs

Maintenance and Sustainment Costs

The use of FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, as described in FEMA Policy FP 205- 402-125-1, Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants, located at: <http://www.fema.gov/media-library/assets/documents/32474>), unless otherwise noted.

Grant funds are intended to support the National Preparedness Goal (the Goal) and fund projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients the ability to meet this objective, the policy set forth in [IB 379: Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#) allows for the expansion of eligible maintenance and sustainment costs which must be in (1) direct support of existing capabilities; (2) must be an otherwise allowable expenditure under the applicable grant program, and (3) be tied to one of the core capabilities in the five mission areas outlined in the Goal. Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either federal grant or any other source of funding other than DHS/FEMA preparedness grant program dollars.

Bonds

Financial markets are not always predictable, and commercial suppliers are not always reliable; but there are options to provide resource contingencies to support an IBSGP award.

- **Prepayment Bond:** Prepayment Bonds provide a measure of economic security for an organization that is going to advance funds to a vendor(s). The prepayment bond generally may be obtained through the vendor or bank. The prepayment bond protects funds in the event a vendor fails to perform (e.g., not finishing/delivering contracted service/equipment, or going out of business). Prepayment bonds are chargeable to an award.
 - **Encouraged Prepayment Bond:** Recipients are strongly recommended, but not required, to obtain a prepayment bond for awarded acquisition activities that exceed the Simplified Acquisition Threshold (SAT) (currently \$250,000, but the applicable dollar threshold will be the SAT amount in place at the time of procurement) when recipients are contractually required to advance a down payment and when such advances contain no federal funds (only local funds).
 - **Required Prepayment Bond:** Per 2 C.F.R. § 200.304(b), recipients are required to obtain a prepayment bond for awarded acquisition activities that exceed the SAT; a prepayment bond is required when recipients are contractually required to advance a

down payment and when such advances contain only federal funds or a combination of federal and local funds.

- **Fidelity Bond:** Reasonable costs of fidelity bonds (or like insurance as provided for by applicable state or tribal laws) covering the maximum amount of IBSGP funds the officer, official, or employee handles at any given time for all personnel who disburse or approve disbursement of IBSGP funds may be allowable if required by the terms and conditions of the award or if generally required by the tribe in its general operations. If a fidelity bond is required by a recipient in its general operations, those costs must be charged as indirect costs. *See* 2 C.F.R. § 200.427.

Encouraged Use of Certain Products Produced in the United States

Pursuant to Executive Order 13858 “[Strengthening Buy-American Preferences for Infrastructure Projects](#),” FEMA encourages non-Federal entities under this grant program to use, to the greatest extent practicable and consistent with the law, iron and aluminum as well as steel, cement, and other manufactured products produced in the United States, in projects funded by an award under this grant program affecting surface transportation, including roadways, bridges, railroads, and transit; aviation; ports, including navigational channels; water resources projects; energy production, generation, and storage, including from fossil-fuels, renewable, nuclear, and hydroelectric sources; electricity transmission; gas, oil, and propane storage and transmission; electric, oil, natural gas, and propane distribution systems; broadband internet; pipelines; stormwater and sewer infrastructure; drinking water infrastructure; and cybersecurity. Notwithstanding this encouragement, non-Federal entities must take care that all procurements and contract actions are consistent with law, the Preparedness Grants Manual and applicable appendices, the grant program’s NOFO, and the Federal procurement standards at 2 C.F.R. §§ 200.317-200.326.

Program Appendix F:

Intercity Passenger Rail (IPR) Program

The IPR grant recipient may only use IPR grant funds for the purposes set forth in the NOFO, and all investments must be consistent with the statutory authority for the award. Grant funds may not be used for matching funds for other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, Federal funds may not be used to sue the Federal Government or any other government entity.

Applicable Regulations

Costs charged to a an IPR award must be consistent with the uniform administrative requirements and audit requirements for Federal awards, located at 2 C.F.R. Part 200, Subparts A-D and F. For more information on 2 C.F.R. Part 200, please see IB 400 at https://www.fema.gov/media-library-data/1419366341862-296dd0cc30bbf64a6b45581afe9d8b17/InformationBulletin400_2CFERPart200_FINAL.pdf. Costs charged to an IPR 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.

IPR Priorities

See the annual IPR NOFO.

Allowable Costs

Specific investments made in support of the funding priorities discussed in the annual IPR NOFO generally fall into one of the following six allowable expense categories:

- 1) Planning
- 2) Operational Activities
- 3) Equipment and Capital Projects
- 4) Training and Awareness Campaigns
- 5) Exercises
- 6) Management and Administration

The following provides guidance on allowable costs within each of these areas:

Planning

Planning activities that address the Soft Targets/Crowded Places; Cybersecurity; and Emergent Threats Priorities.

IPR funds may be used for the following types of planning activities:

- Development and enhancement of system-wide security risk management plans, to include cyber;

- Development or further strengthening of continuity of operations plans, response plans, station action plans, risk assessments, and asset-specific remediation plans;
- Development or further strengthening of security assessments, including multi-agency and multi-jurisdictional partnerships and conferences to facilitate planning activities;
- Hiring of full or part-time staff and contractors or consultants to assist with planning activities only to the extent that such expenses are for the allowable activities within the scope of this grant (not for the purpose of hiring public safety personnel);
- Materials required to conduct planning activities; and
- Other project planning activities, with prior approval from DHS/FEMA.

Operational Activities

Operational Activities that address the Soft Targets/Crowded Places; and Emergent Threat Priorities.

DHS/FEMA encourages applicants to develop innovative operational approaches to enhance the security of transit systems. Projects that use visible, unpredictable deterrence, including operational packages dealing with explosive detection canine teams, mobile screening teams, and anti-terrorism teams, directly support enhancing the protection of soft targets and crowded places. Implementation of one of the three Operational Package (OPack) models discussed below complements existing security systems and provides an appropriate, practical, and cost-effective means of protecting assets.

Agencies may submit IJs to fund transit security police forces/law enforcement providers for patrols and activities on overtime, such as directed patrols, additional canine teams, mobile screening teams, or anti-terrorism team patrols. These activities must be dedicated to the transit environment and must be anti-terrorism in nature. Agencies must identify the type of activity, length of operation (hours), number of personnel, and cost based on length of operation and personnel. Agencies should also provide a risk-based justification for the request, including linkage to a known event, such as hosting a significant regional sporting or political event; or a period of heightened awareness, such as a national holiday. Three OPack types have been developed to support operational activities and are available for funding under the IPR:

- **Explosives Detection Canine Teams (EDCTs).** When combined with the existing capability of a transit security/police force, the added value provided through the addition of an EDCT is significant. EDCTs are a proven, reliable resource to detect explosives and a key component in a balanced counter-sabotage program. IPR funding will provide funds to establish dedicated security/police force canine teams. Each canine team will be composed of one dog and one handler.
- **Anti-Terrorism Teams (ATTs).** The ATT capability provided through IPR funding is for uniformed, dedicated transit patrols on a normal operational basis, rather than using teams only for a surge capacity as provided by DHS/FEMA in the past. ATTs do not supersede other local transit security forces; rather, they augment current capabilities. Each ATT will consist of four individuals, including two overt elements (*e.g.*, uniformed transit sector law enforcement officer, canine team, mobile explosive screeners), and two discreet observer elements.
- **Mobile Explosive Screening Teams (MESTs).** The MEST OPack will allow recipients the flexibility to deploy combinations of trained individuals and technologies that will assist in making screening decisions where there are large numbers of individuals with hand-carried items. This screening technology will be coupled with mobile explosive screening technologies.

Note: Funds for canine teams may not be used to fund drug detection and apprehension technique training. Only explosives detection training for the canine teams will be funded.

Five-Year Security Capital Plan and Operational Sustainment

Applicant requests for OPack funding must include the submission of a Five-Year Security Capital and Operational Sustainment Plan in ND Grants. This plan must include how the agency proposes to implement capital projects and demonstrate how the agency will sustain the operational investments (including officers hired with federal funding) and capabilities after grant funding has been expended. ***Requests for OPacks will not be funded if the applicant does not have and submit a Security Capital and Operational Sustainment Plan.***

Funding Availability for OPacks

OPacks have the potential to be funded for up to a 36-month period from the award date. The monetary figures presented below are stated in terms of cost per period of performance (which indicates actual/complete funding for a 36-month period). Additionally, any OPack costs after the period of performance (including expenses related to the maintenance, personnel, equipment, etc.) are the responsibility of the applicable transit system. Additional funding may be applied for in future grant cycles to maintain this operational capability, but future funding is not guaranteed and requires approval. If these positions are not sustained, the public transportation agency may not be eligible for this personnel support in the future. The table below identifies the maximum funding available for the different OPack types.

Available Funding for OPacks

Operational Package	Maximum Funding per Year (12 months)	Maximum Funding per Period of Performance (36 months)
EDCT	\$150,000 per team	\$450,000 per team
ATT	\$500,000 per team	\$1,500,000 per team
MEST	\$600,000 per team	\$1,800,000 per team

OPack Requirements

IPR OPack funds may be used for new positions or to sustain existing capabilities/programs (e.g., canine teams) already supported by the recipient. Applicants pursuing both new OPacks and sustainment funding for existing OPacks must indicate in their IJs which funding the higher priority for their agency is. Additionally, applicants must provide the number of existing teams (EDCT, ATT, and MEST) already in place, regardless of how they are funded. The below table identifies specific OPack requirements.

OPack Requirements

Operational Package	Requirements
Explosives Detection Canine Teams	Please refer to the pages below for detailed information regarding EDCTs under the IPR

Operational Package	Requirements
Anti-Terrorism Teams	<p>Specific for the Canine Team within the ATT:</p> <ul style="list-style-type: none"> • Each canine team, composed of one dog and one handler, must be certified by an appropriate, qualified organization • Canines should receive an initial basic training course and also weekly maintenance training sessions thereafter to maintain the certification • The basic training averages 10 weeks for the team, 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 United States Police Canine Association (USPCA), or the International Explosive Detection Dog Association (IEDDA) may be used to meet this requirement • The individuals hired for the covert and overt elements must be properly trained law enforcement officers • Certifications should be on file with the recipient and must be made available to DHS/FEMA upon request
Mobile Explosives Screening Team	Certifications should be on file with the recipient and must be made available to DHS/FEMA upon request

Allowable Expenses for OPacks

The table below identifies allowable expenses for the various OPacks. Please see the accompanying notes for clarification of certain allowable costs.

Allowable Expenses for OPacks

Operational Package		Salary and Fringe Benefits	Training and Certification	Equipment Costs	Purchase and Train a Canine	Canine Costs ^b
1)	EDCT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> ^c	<input type="checkbox"/>
2)	ATT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3)	Mobile Explosives Screening Team	<input type="checkbox"/>		<input type="checkbox"/> ^d		
<p>^a Travel costs associated with training for personnel, handlers, and canines are allowable</p> <p>^b Canine costs include but are not limited to a canine's veterinary, housing, and feeding costs</p> <p>^c One type of allowable training is training specific to the detection of common explosives odors</p> <p>^d Equipment and other costs can include but are not limited to explosives detection; stainless steel search tables; consumables such as gloves, swabs, and alcohol; and land mobile radios</p>						

Specific Guidance on Explosive Detection Canine Teams (EDCT)

EDCT Certification

Each 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 September 14, 2007, in addition to the requirements set forth in the NOFO.

EDCT 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 DHS/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 IPR-funded EDCTs are not available, other, non-IPR 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 4 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 DHS/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 of time, 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.
- 8) The recipient will ensure that adequate routine and emergency veterinary care are provided for all canines.

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

Equipment and Capital Projects

Equipment and Capital Projects that address the Soft Targets/Crowded Places; Cybersecurity; and Emergent Threats Priorities.

Priority projects include Top Transit Asset List risk remediation and protection of other high-risk, high-consequence areas or systems that have been identified through system-wide risk assessments:

- Projects related to physical security enhancements at rail and bus stations in UASI jurisdictions, including security cameras, security screening equipment for people and baggage, and access control (e.g., fences, gates, barriers, etc.).
- Projects related to cybersecurity of access control, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls, etc. or passenger/vehicle/cargo security screening equipment support. Cybersecurity assessments are allowable.

Equipment Acquisition

IPR funds may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found in the [DHS Authorized Equipment List \(AEL\)](#). These costs include:

- Personal protection equipment
- Explosive device mitigation and remediation equipment
- Chemical, biological, radiological, nuclear, and high explosive (CBRNE) operational search and rescue equipment, logistical support equipment, reference materials, or incident response vehicles
- Interoperable communications equipment
- Components or systems needed to address flaws in the computerized systems that control generators, switching stations, and electrical substations as well as other emerging threats to infrastructure critical to the U.S. economy
- Detection Equipment
- Power equipment
- Terrorism incident prevention equipment
- Physical security enhancement equipment

Unless otherwise noted, equipment must be certified as meeting required regulatory and DHS/FEMA-adopted standards to be eligible for purchase using IPR funds. Equipment must comply with the *Occupational Safety and Health Act* requirement for certification of electrical equipment by a nationally recognized testing laboratory and demonstrate compliance with relevant DHS/FEMA-adopted standards through a supplier's declaration of conformity with appropriate supporting data and documentation per International Organization for Standardization/International Electro-technical Commission (ISO/IEC) 17050, Parts One and Two. The recipient must have all necessary certifications and licenses for the requested equipment, as appropriate, prior its purchase. In addition, if the recipient is using IPR funds to support emergency communications equipment activities must comply with the *SAFECOM Guidance for Emergency Communication Grants*, including provisions on technical standards that ensure and enhance interoperable communications. This *SAFECOM* Guidance can be found at: <https://www.dhs.gov/safecom>.

Requirements for Small Unmanned Aircraft Systems

All requests to purchase Small Unmanned Aircraft Systems (SUAS) with DHS/FEMA grant funding must comply with [Information Bulletin \(IB\) 426](#) and must include a description of the policies and procedures

that the recipient, as the entity that will purchase, take title to, or otherwise use the SUAS equipment, has in place to safeguard individuals' privacy, civil rights, and civil liberties.

Cybersecurity Projects

IPR funds may be used for projects that enhance the cybersecurity of:

- Access controls, sensors; security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls (such as firewalls, network segmentation, predictive security cloud, etc.)
- Passenger/vehicle/cargo security screening equipment (cybersecurity assessments are allowable)

When requesting funds for cybersecurity, applicants are encouraged to propose projects that would aid in implementation of all or part of the [Framework for Improving Critical Infrastructure Cybersecurity](#) (the "Framework"), developed by the National Institute of Standards and Technology (NIST). The Framework gathers existing international standards and practices to help organizations understand, communicate, and manage their cyber risks. For organizations that do not know where to start with developing a cybersecurity program, the Framework provides initial guidance. For organizations with more advanced practices, the Framework offers ways to improve their programs, such as through better communication with their leadership and suppliers about management of cyber risks.

DHS's Critical Infrastructure Cyber Community C³ Voluntary Program also provides resources to critical infrastructure owners and operators to assist in adoption of the Framework and managing cyber risks. Additional information on the Critical Infrastructure Cyber Community C³ Voluntary Program can be found at www.dhs.gov/ccubedvp.

DHS's Enhanced Cybersecurity Services (ECS) program is an example of a resource that assists in protecting U.S.-based public and private entities and combines key elements of capabilities under the "Detect" and "Protect" functions to deliver an impactful solution relative to the outcomes of the Framework. Specifically, ECS offers intrusion prevention and analysis services that help U.S.-based companies and SLTT governments defend their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sourcing timely, actionable cyber threat indicators from sensitive and classified Government Furnished Information. DHS then shares those indicators with accredited Commercial Service Providers (CSPs). Those CSPs in turn use the indicators to block certain types of malicious traffic from entering a company's networks. Groups interested in subscribing to ECS must contract directly with a CSP in order to receive services. Please visit <http://www.dhs.gov/enhanced-cybersecurity-services> for a current list of ECS CSP points of contact.

Capital (Construction) Projects Guidance

The recipient must obtain written approval from FEMA prior to the use of any IPR 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, any other locally required planning permits. Additionally, the recipient is required to submit a SF-424C and budget detail citing the project costs.

The recipient is also 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 the relevant Historic Preservation Office to identify potential historic preservation issues and to discuss the potential for project effects; compliance with all state and 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](#), EHP Directive and Instruction, [FEMA Directive 108-1](#), and [FEMA Instruction 108-1-1](#), must also be identified to the FEMA HQ Program Analyst within the first six months of the award, regardless of the length of the period of performance. Completed EHP review materials for construction and communication tower projects must be submitted no later than 12 months before the end of the period of performance. EHP review materials should be sent to gpdehpinfo@fema.gov.

If the recipient uses funds for construction projects, it must comply with the *Davis-Bacon Act* (codified as amended at 40 U.S.C. §§ 3141 *et seq.*). It must ensure that its 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 the Department of Labor (DOL) wage determinations, is available at <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Training and Awareness Campaigns

Training and Awareness Campaigns that address the Soft Targets/Crowded Places; Cybersecurity; and Emergent Threats Priorities.

Training

IPR funds may be used for the following training activities:

- **Training Topics.** Priority topics include active shooter training, security training for employees, and public awareness/preparedness campaigns.
- **Training Workshops.** Grant funds may be used to plan and conduct training workshops, including costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel, and training plan development. The recipient is strongly encouraged to use free public space, locations, or facilities, whenever available, prior to the rental of space, locations, or facilities. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. Any training or training gaps, including those for children and individuals with disabilities or access and functional needs, should be identified in an After-Action Report/Improvement Plan (AAR/IP) and addressed in the training cycle.
- **Hiring of Full or Part-Time Staff or Contractors/Consultants.** Full or part-time staff or contractors/consultants may be hired to support training-related activities. Reimbursement of these costs should conform with the policies of recipient, as well as any applicable Federal and DHS/FEMA policies, rules, and regulations. Dual compensation is unallowable, in other words, an employee of a unit of government may not receive compensation from their unit or agency of government and from an award for a single period of time (*e.g.*, 1:00 p.m. to 5:00 p.m.), even though such work may benefit both activities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for allowable activities within the scope of the grant.
- **Overtime and Backfill Costs.** The entire amount of overtime costs, including payments related to backfilling personnel, that are the direct result of attendance at FEMA and approved training courses and programs are allowable. Reimbursement of these costs should follow the policies of the recipient, as well as any applicable Federal and DHS/FEMA policies, rules, and regulations. Dual compensation is never allowable.

- **Travel.** Domestic travel costs (e.g., airfare, mileage, per diem, and hotel) are allowable as expenses by employees who are on travel status for official business related, approved training, subject to the restrictions at 2 C.F.R. Part 200. International travel is not an allowable expense.
- **Supplies.** Supplies, items that are expended or consumed during the course of the planning and conduct of the training project(s) (e.g., gloves and non-sterile masks), are allowable expenses.
- **Funds Used to Develop, Deliver, and Evaluate Training.** Funds used to develop, deliver, and evaluate training, including costs related to administering the training, planning, scheduling, facilities, materials and supplies, reproduction of materials, and equipment are allowable expenses. Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. Any training or training gaps, including those for children and individuals with disabilities or access and functional needs, should be identified in the AAR/IP and addressed in the training cycle.

Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model of instructional design. Information on DHS/FEMA-approved training can found at <http://www.firstrespondertraining.gov/>.

Awareness Campaigns

IPR funds may be used for the development and implementation of awareness campaigns to raise public awareness of indicators of terrorism and terrorism-related crime and for associated efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. DHS currently sponsors or supports a number of awareness campaigns. Please review materials, strategies, and resources at <https://www.dhs.gov/dhs-campaigns> before embarking on the development of an awareness campaign for local constituencies and stakeholders.

Note: DHS requires that all public and private sector partners wanting to implement and/or expand the DHS “If You See Something, Say Something®” campaign (“campaign”) using grant funds work directly with the DHS Office of Partnership and Engagement (OPE). This will help ensure that the awareness materials (e.g., videos, posters, tri-folds, etc.) remain consistent with DHS’s messaging and strategy for the campaign and compliant with the initiative’s trademark, which is licensed to DHS by the New York Metropolitan Transportation Authority. Coordination with OPE, through the campaign’s office (seesay@hq.dhs.gov), must be facilitated by the FEMA Program Analyst.

Exercises

Exercise activities that address the Soft Targets/Crowded Places; Cybersecurity; and Emergent Threats Priorities.

IPR funds may be used for the following exercise activities:

- **Funds Used to Design, Develop, Conduct and Evaluate an Exercise.** This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low-risk setting. Any shortcomings or gaps identified, including those for children and individuals with disabilities or access and functional needs, should be identified in an effective corrective action program that includes development of improvement plans that are dynamic documents, with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

- **Hiring of Full or Part-Time Staff or Contractors/Consultants.** Full or part-time staff may be hired to support exercise-related activities. Reimbursement of these costs should conform with the policies of the recipient, as well as any applicable Federal and DHS/FEMA policies, rules, and regulations. Dual compensation is not allowable, meaning, in other words, that an employee of a unit of government may not receive compensation from their unit or agency of government and from an award for a single period of time (*e.g.*, 1:00 p.m. to 5:00 p.m.), even though their work may benefit both entities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant. The recipient must follow all applicable procurement regulations at 2 C.F.R. Part 200 when procuring contractor services.
- **Overtime and Backfill Costs.** The entire amount of overtime costs, including payments related to backfilling personnel, which are the direct result of time spent on designing, developing, and conducting exercises are allowable expenses. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the recipient and has the approval of the awarding agency, if applicable. Dual compensation is never allowable.
- **Travel.** Domestic travel costs are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of exercise project(s), subject to the restrictions at 2 C.F.R. Part 200. International travel costs are not allowable expenses.
- **Supplies.** Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (*e.g.*, gloves, non-sterile masks, and disposable protective equipment).
- **Other Items.** These costs include the rental of space or locations for exercise planning and executing, rental of equipment, etc. The recipient is encouraged to use free public space, locations, or facilities, whenever available, prior to the rental of space, locations, or facilities. These also include costs that may be associated with inclusive practices and the provision of reasonable accommodations and modifications to provide full access for children and adults with disabilities.

Management and Administration (M&A)

Management and administration costs are allowed under this program. M&A costs are activities directly related to managing and administering the award. The recipient may use up to 5% of the amount of the award for its M&A costs.

Current fiscal year IPR funds may be used for the following M&A costs:

- Hiring of full-time or part-time staff, including contractors and consultants, to execute the following:
 - Management of the current fiscal year IPR Award
 - Design and implementation of the current fiscal year IPR submission meeting compliance with reporting/data collection requirements, including data calls
- Information collection and processing necessary to respond to DHS/FEMA data calls
- Domestic travel expenses related to IPR grant administration, in compliance with the Super Circular, 2 C.F.R. Part 200.
- Acquisition of authorized office equipment, including personal computers or laptops for IPR M&A purposes.

Indirect Costs

Indirect costs are allowable under this program as described in the Federal Acquisition Regulations (FAR).

Unallowable Costs

Specific unallowable costs include:

- ***Grant funds must comply with [IB 426](#) and may not be used for the purchase of the following prohibited equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.*** Expenditures for items unrelated to grant allowable activities, such as general-use software, general-use computers and related equipment (other than for allowable M&A activities or for other associated preparedness or response functions), general-use vehicles, licensing fees, weapons systems, and ammunition are also prohibited.
- Personnel costs (except as detailed above or otherwise allowed by statute).
- Activities unrelated to the completion and implementation of the IPR program.
- Other items not in accordance with the Authorized Equipment List (AEL) or not previously listed as allowable costs.
- Costs related to any matching or cost share requirement for any other Federal award
- Costs related to lobbying or intervention in Federal regulatory proceedings
- Costs related to suing the Federal Government or any other government entity
- Pre-award costs, unless approved in writing by DHS/FEMA and included in the grant award
- Costs that are not consistent with the Cost Principles located in FAR 31.2, as applicable

Maintenance and Sustainment Costs

The use of FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, as described in FEMA Policy FP 205-402-125-1, *Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants*, located at <http://www.fema.gov/media-library/assets/documents/32474>), under all active and future grant awards, unless otherwise noted.

Grant funds are intended to support the National Preparedness Goal and to fund projects that build and sustain the core capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. In order to provide recipients with the ability to meet this objective, the policy set forth originally in [IB 379: Guidance to State Administrative Agencies to Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#) allows for the expansion of eligible maintenance and sustainment costs that must be (1) in direct support of existing capabilities, (2) an otherwise allowable expenditure under the applicable grant program, and (3) tied to one of the core capabilities in the five mission areas outlined in the Goal. Additionally, eligible costs may also be in support of equipment, training, and critical resources that have previously been purchased with either Federal grant or any other source of funding other than DHS/FEMA preparedness grant program dollars.

Encouraged Use of Certain Products Produced in the United States

Pursuant to Executive Order 13858 “[Strengthening Buy-American Preferences for Infrastructure Projects](#),” FEMA encourages non-federal entities under this grant program to use, to the greatest extent

practicable and consistent with the law, iron and aluminum as well as steel, cement, and other manufactured products produced in the United States, in projects funded by an award under this grant program affecting surface transportation, including roadways, bridges, railroads, and transit; aviation; ports, including navigational channels; water resources projects; energy production, generation, and storage, including from fossil-fuels, renewable, nuclear, and hydroelectric sources; electricity transmission; gas, oil, and propane storage and transmission; electric, oil, natural gas, and propane distribution systems; broadband internet; pipelines; stormwater and sewer infrastructure; drinking water infrastructure; and cybersecurity. Notwithstanding this encouragement, non-federal entities must take care that all procurements and contract actions are consistent with law, the Preparedness Grants Manual and applicable appendices, the grant program's NOFO, and the federal procurement standards at 2 C.F.R. §§ 200.317-200.326.

Program Appendix G: Port Security Grant Program (PSGP)

PSGP grant recipients and subrecipients may only use PSGP grant funds for the purposes set forth in the NOFO, and all investments must be consistent with the statutory authority for the award. These grant funds may not be used for matching funds for other federal awards, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity.

Applicable Regulations

Costs charged to a PSGP 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. For more information on 2 C.F.R. Part 200, please visit https://www.fema.gov/media-library-data/1419366341862-296dd0cc30bbf64a6b45581afe9d8b17/InformationBulletin400_2CFERPart200_FINAL.pdf.

PSGP Priorities

See the annual PSGP NOFO.

Limitations on Funding

As part of the PSGP application process, applicants must complete the approved [Investment Justification \(IJ\) template](#) provided addressing each initiative being proposed for funding. A separate IJ should be submitted for each proposed project which should represent the complete scope of work and materials required to achieve a single overall capability. For example, a project could be to procure a boat specifically designed and equipped as Chemical, Biological, Radiological, Nuclear and High-Yield Explosives (CBRNE) detection, prevention, response, and/or recovery platform. The IJ for this example project should include the CBRNE equipment in the same IJ as the vessel.

In accordance with 46 U.S.C. § 70107(b)(2), PSGP funding for projects for the cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers **cannot exceed \$1 million federal share per project.**

The \$1 million per project limitation applies only to those projects funded under 46 U.S.C. § 70107(b)(2) and does not apply to projects funded under other provisions of Section 70107.

Allowable Direct Costs

Specific investments made in support of the funding priorities discussed in the annual PSGP NOFO generally fall into one of the following six allowable expense categories:

- Planning
- Operational Activities
- Equipment and Capital Projects

- Training and Awareness Campaigns
- Exercises
- Management and Administration

The following provides guidance on allowable costs within each of these areas:

Planning

Planning activities address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Planning Priorities.

PSGP funds may be used for the following types of planning activities:

- Development or updating of port wide risk mitigation plan (PRMP), including the conducting of port security vulnerability assessments as necessary to support plan update/development
- Development and enhancement of security plans and protocols within the Area Maritime Security Plan (AMSP), PRMP, and the Business Continuity and Resumption of Trade Plans (BCRTP) in support of maritime security and risk mitigation planning
- Materials required to conduct planning activities
- Travel and per diem related to the professional planning activities noted in this section
- Other port wide project planning activities, which emphasize the ability to adapt to changing conditions and be prepared to withstand, and recover from, disruptions due to emergencies with prior approval from DHS/FEMA

Backfill, overtime, hiring of part-time temporary personnel, and contractors or consultants to assist with planning activities. Copies of PSGP-funded plans must be made available to FEMA and USCG upon request.

Operational Activities

Operational Activities address the Soft Targets/Crowded Places; and Emergent Threat Priorities.

Explosive Detection Canine Teams (EDCTs)

Use of canines (K-9) for explosive detection is one of the most effective solutions for the detection of vehicle-borne IEDs. When combined with the existing capability of a port or ferry security/police force, the added value provided through the addition of a canine team is significant. EDCTs are a proven, reliable resource to detect explosives and are a key component in a balanced counter-sabotage program. Eligibility for funding of EDCTs is restricted to:

- U.S. Ferry Systems regulated under 33 C.F.R. Parts 101, 103, 104, and the passenger terminals these specific ferries service under 33 C.F.R. Part 105
- Maritime Transportation Security Act (MTSA) regulated facilities
- Port authorities, port police, and local law enforcement agencies that provide direct layered security for these U. S. Ferry Systems and MTSA-regulated facilities, and are defined in an Area Maritime Security Plan (AMSP), Facility Security Plan (FSP), or Vessel Security Plan (VSP)

Applicants may apply for up to \$450,000 (\$150,000/year for three years) per award to support this endeavor. At the end of the grant period (36 months), recipients will still be responsible for continuing the heightened level of capability provided by the EDCT. **A sustainment plan must be submitted with the applicant's IJ to address the 12-month period beyond the period of performance of the award.**

Eligible EDCT Costs

Funds for these EDCTs may **not** be used to fund drug detection and apprehension technique training. Only explosives detection training for EDCTs will be funded. The PSGP EDCT funds may only be used for **new or expanded** capabilities/programs and cannot be used to pay for existing K-9 teams, personnel, or K-9 training costs already supported by the port area. Repair and replacement of existing EDCT equipment is allowed. Eligible costs include:

- Contracted K-9 and handler providing services in accordance with PSGP guidance
- Salary and fringe benefits of new full- or part-time K-9 handler positions
- Training and certifications (travel costs associated with training for new or expanded full or part time agency handlers, and canines are allowable)
- K-9 and handler equipment costs
- Purchase and train a new K-9 and handler for CBRNE detection
- K-9 maintenance costs (K-9 costs include but are not limited to: veterinary, housing, and feeding costs)

Ineligible EDCT costs include, but are not limited to:

- Hiring costs, including costs associated with initial police academy training of new officers
- Meals and incidentals associated with travel for initial certification
- Vehicles modified to be used solely to transport canines

EDCT Certification

Each EDCT, composed of one dog and one handler, must be certified by an appropriate, qualified organization. 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 10 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 DHS/FEMA upon request.

EDCT Submission Requirements

Successful applicants will be required to submit an amendment to their approved VSP or FSP per 33 C.F.R. Parts 104 and/or 105 detailing the inclusion of a K-9 explosive detection program into their security measures. The recipient will ensure that a written plan or SOPs exist that describe EDCT deployment policy to include visible and unpredictable deterrent efforts and on-call EDCTs rapid response times as dictated by the agency's FSP or VSP. The plan or SOPs must be made available to DHS/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 EDCT Resources Available for K-9 Costs

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

Organization Costs

Allowable organization-related costs are limited to those activities associated with new and ongoing maritime security operations essential to the national priorities. All such activities must be focused exclusively on maritime security and coordinated with the local COTP. PSGP funding used for organizational costs will only fund immediate needs for personnel that will be directly engaged in maritime security activities. Allowable organization personnel costs include:

- **Backfill, Overtime, Hiring of Full or Part-Time Personnel or Contractors/Consultants.** Full or part-time staff or contractors/consultants may be hired to support training-related and/or maritime-security-related activities conducted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant. Salary and fringe benefit payments must be in accordance with the policies of the state or unit(s) of local government and have the approval of the state or awarding agency. Dual compensation is not allowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government AND from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both activities. Limitations may apply for grant related activities. See specific guidance provided within this Manual for additional details on allowable organization costs (i.e., Training – Personnel costs are limited to backfill and overtime).
- **Hiring new, full-time personnel to:**
 - Operate maritime security patrol vessels (first response agencies only)
 - Staff a new or expanded interagency maritime security operation center
 - Support maritime security/counterterrorism efforts in the local Joint Terrorism Task Force (JTTF) center
 - Support credentialing access to a MTSA facility
- **Backfill and Overtime costs for existing personnel to:**
 - Operate patrol vessels in support of pre-planned, mission critical activities, as identified by the local COTP (not including routine patrol)
 - Attend approved maritime security training courses
- **Personnel or contracted costs to:**
 - Install, repair, and replace port security equipment acquired with DHS/FEMA preparedness grant funds. Note this does not include routine maintenance, such as oil changes and daily/weekly systems tests.
- **Contracted costs to:**
 - Provide approved training courses
 - Provide warranty, maintenance, and service agreements for equipment purchased under this grant

Organization costs will only be funded to address port (or facility) security needs as outlined in the NOFO and this appendix. PSGP funding for new permanent or part-time personnel will not exceed the 36-month period of performance. Applicants must provide reasonable assurance that personnel costs can be sustained beyond the 36-month award period. **A sustainment plan must be submitted with the applicant's IJ to address the 12-month period beyond the period of performance of the award.**

Equipment and Capital Projects

Equipment and Capital Projects address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Equipment/Capital Projects Priorities.

Equipment Acquisition

PSGP funds must comply with IB 426. PSGP funds may be used for the following categories of equipment. A comprehensive listing of allowable equipment categories and types is found in the [DHS Authorized Equipment List \(AEL\)](#). Requests for vehicles of any type are subject to secondary review and approval by the National Review Panel. These costs include:

- Personal Protective Equipment (PPE) for maritime security providers, such as ballistic protective body armor (not including uniforms)
- CBRNE response and remediation equipment for maritime security providers
- CBRNE decontamination equipment for direct maritime security providers and MTSA-regulated industry
- CBRNE detection-equipped patrol vehicles (**not including armored personnel carriers or tow trucks**), provided they will be used exclusively for port/facility CBRNE detection security operations. A CBRNE detection equipped patrol vehicle must include specifically identified, permanently mounted detection equipment.
- Mobile Command Centers only when validated by the COTP as essential to address a specifically required capability outlined in the approved AMSP.
- CBRNE detection equipped and patrol watercraft vessel/small boat used to directly support maritime security for a facility or within a Port Area on a routine basis (CBRNE detection equipment requested with the watercraft/small boat in the IJ must be listed and also detailed in the budget). However, a vessel is not required to be CBRNE equipped.
- Marine firefighting vessels, provided they are outfitted with CBRNE detection equipment and are designed and equipped to meet NFPA 1925: Standard on Marine Fire-Fighting Vessels
- Firefighting foam and Purple-K Powder (PKP) may be purchased by public fire departments that have jurisdictions in a port area and would respond to an incident at an MTSA regulated facility. MTSA facilities may also receive funding for this purpose. Funding will be limited to a one-time purchase based on a worst-case incident at the facility or facilities
- Information-sharing technology; components or equipment designed to share maritime security risk information and maritime all-hazards risk information with other agencies (equipment must be compatible with generally used equipment)
- Maritime security risk mitigation interoperable communications equipment
- Terrorism incident prevention and response equipment for maritime security risk mitigation
- Physical security enhancements, to include TWIC projects (e.g. card readers, fences, blast resistant glass, turnstiles, hardened doors and vehicle gates) at maritime facilities
- Portable fencing, CCTVs, passenger vans, mini-buses, etc. to support secure passage of vessel crewmembers through a MTSA regulated facility
- Equipment in support of resiliency, such as interoperable communications, intrusion prevention/detection, physical security enhancements, and software and equipment needed to support essential functions during a continuity situation
- Generators with appropriate capability (size) to provide back-up power to systems and equipment that support Maritime Domain Awareness (not including routine operational capabilities):
 - Access control equipment and systems
 - Detection and security surveillance equipment
 - Enhancement of Command and Control facilities

- Equipment for new personnel, such as personal protective equipment, is an allowable expense. Weapons and equipment associated with weapons maintenance/security (e.g., firearms, ammunition, and gun lockers) are not allowable.

Requirements for Small Unmanned Aircraft Systems

All requests to purchase Small Unmanned Aircraft Systems (SUASs) with FEMA grant funding must comply with [IB 426](#) and must include a description of the policies and procedures the jurisdiction that will purchase, take title to, or otherwise use the SUAS equipment has in place to safeguard individuals' privacy, civil rights, and civil liberties.

Sonar Devices

The four types of allowable sonar devices are: imaging sonar, scanning sonar, side scan sonar, and three-dimensional sonar. These types of sonar devices are intended to support the detection of underwater improvised explosive devices and enhance maritime domain awareness. The eligible types of sonar, and short descriptions of their capabilities, are provided below:

- 1) **Imaging Sonar:** A high-frequency sonar that produces “video-like” imagery using a narrow field of view. The sonar system can be pole-mounted over the side of a craft or hand-carried by a diver.
- 2) **Scanning Sonar:** Consists of smaller sonar systems that can be mounted on tripods and lowered to the bottom of the waterway. Scanning sonar produces a panoramic view of the surrounding area and can cover up to 360 degrees.
- 3) **Side Scan Sonar:** Placed inside a shell and towed behind a vessel. Side scan sonar produces strip-like images from both sides of the device.
- 4) **Three-Dimensional Sonar:** Produces 3-dimensional imagery of objects using an array receiver.

Maritime Domain Awareness

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.” Homeland Security Presidential Directive-13 (NSPD-41/HSPD-13) (Maritime Security Policy, December 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. Applicants are encouraged to familiarize themselves with this National Strategy.

IED and CBRNE Prevention, Protection, Response, Recovery Capabilities

Port areas should continue to enhance their capabilities to prevent, detect, respond to and recover from terrorist attacks employing IEDs, CBRNE devices, and other non-conventional weapons. Please refer to DHS, Small Vessel Security Strategy (Apr. 2008), available at http://www.dhs.gov/files/publications/gc_1209408805402.shtm.

Physical Security

Physical security is security measures that are designed to deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems and techniques. Physical security has been a focus of PSGP since the program's inception in 2002. Primarily, physical security is intended to harden MTSA-regulated facilities against attacks. Law enforcement may contribute to physical security through patrols, however, patrol vessels generally enhance multiple core capabilities with a focus on CBRNE detection, deterrence, and response. Funding through PSGP for physical security projects should be only directed toward those projects that address identified MTSA required activities and identified in the entity FSP and/or the port area AMSP. Some examples of funded projects include TWIC-related equipment, fencing, lighting, gates, and closed-circuit television (CCTV).

Cybersecurity Projects

PSGP funds may be used for projects that enhance the cybersecurity of: access controls; sensors; security cameras; badge/ID readers; ICS/SCADA systems; process monitors and controls (such as firewalls, network segmentation, predictive security cloud, etc.); and passenger/vehicle/cargo security screening equipment (cybersecurity assessments are allowable). When requesting funds for cybersecurity, applicants are encouraged to propose projects that would aid in implementation of all or part of the [Framework for Improving Critical Infrastructure Cybersecurity](#) (the "Framework") developed by the National Institute of Standards and Technology (NIST). The Framework gathers existing international standards and practices to help organizations understand, communicate, and manage their cyber risks. For organizations that do not know where to start with developing a cybersecurity program, the Framework provides initial guidance. For organizations with more advanced practices, the Framework offers a way to improve their programs, such as better communication with their leadership and suppliers about management of cyber risks.

DHS's Critical Infrastructure Cyber Community C³ Voluntary Program also provides resources to critical infrastructure owners and operators to assist in adoption of the Framework and managing cyber risks. Additional information on the Critical Infrastructure Cyber Community C³ Voluntary Program can be found at www.dhs.gov/ccubedvp. DHS's Enhanced Cybersecurity Services (ECS) program is an example of a resource that assists in protecting U.S.-based public and private entities and combines key elements of capabilities under the "Detect" and "Protect" functions to deliver an impactful solution relative to the outcomes of the Cybersecurity Framework. Specifically, ECS offers intrusion prevention and analysis services that help U.S.-based companies and SLTT governments defend their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sourcing timely, actionable cyber threat indicators from sensitive and classified Government Furnished Information (GFI). DHS then shares those indicators with accredited Commercial Service Providers (CSPs). Those CSPs in turn use the indicators to block certain types of malicious traffic from entering a company's networks. Groups interested in subscribing to ECS must contract directly with a CSP in order to receive services. Please visit <http://www.dhs.gov/enhanced-cybersecurity-services> for a current list of ECS CSP points of contact.

Cybersecurity projects should address risks to the marine transportation system and/or TSIs outlined in the applicable AMSP or priorities prescribed under applicable FSP or VSP, as mandated under the MTSA or the PRMPs. At the port level, examples of cybersecurity projects include but are not limited to projects that enhance the cybersecurity of access control, sensors, security cameras, badge/ID readers, ICS/SCADA systems, process monitors and controls (such as those that monitor flow rates, valve positions, tank levels, etc.), security/safety of the ship-to-port-to-facility-to-intermodal interface, and systems that control vital cargo machinery at the ship/shore interface (such as cranes, manifolds, loading arms, etc.), and passenger/vehicle/cargo security screening equipment.

Vulnerability assessments are generally not funded under PSGP. However, considering the evolving malicious cyber activity, the relative novelty of cybersecurity as a priority within the program, and the need to adopt best practices included in the voluntary Cybersecurity Framework, vulnerability assessments may be funded as contracted costs. Personnel costs (other than M&A) are not an allowable expense for conducting these assessments.

Copies of completed cybersecurity assessments funded under PSGP that impact the maritime transportation system, lead to a “transportation security incident” (as that term is defined under 46 U.S.C. § 70101(6)), or are otherwise related to systems, personnel, and procedures addressed by the facility and vessel plan shall be made available to DHS/FEMA and/or the local COTP upon request. The results of these cybersecurity assessments may be designated as Sensitive Security Information (SSI) and may be used to inform national maritime cybersecurity assessments.

Where a vulnerability assessment has been completed either through contracts or qualified personnel to identify existing gaps and required mitigation efforts, mitigating projects may be funded that include purchase of equipment, software, and infrastructure designed to harden cybersecurity. Specific questions on conducting vulnerability assessments should be referred to the respective FEMA Program Analyst.

Capital (Construction) Projects Guidance

Recipients must obtain written approval from DHS/FEMA prior to the use of 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 Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. § 5196(j)(9)) (the *Stafford Act*),³ 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. Additional information regarding compliance with the *Davis-Bacon Act*, including Department of Labor wage determinations, is available at <http://www.dol.gov/whd/govcontracts/dbra.htm>.

The following types of construction and renovation projects are allowable under PSGP, provided they address a specific vulnerability or need identified in 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)
- Hardened security fences/barriers at access points

³ While the *Maritime Transportation Security Act of 2002*, as amended, 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.

- Any other building or physical facility that enhances access control to the port/MTSA facility area
- 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 period of performance 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.

Training and Awareness Campaigns

Training and Awareness Campaigns address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Training and Awareness Campaign Priorities.

Training

Port areas should assess their training and qualification requirements and coordinate training needs and qualification requirements of incident response personnel. Funding for personnel training is limited to those courses that are **essential to enhance maritime security** and have been listed in the DHS/FEMA approved course catalog by the DHS/FEMA National Training and Education Division (NTED) or the USCG. Approved courses are listed in the following catalogs maintained by NTED: NTED Course Catalog, Federal Sponsored Course Catalog, and the State Sponsored Course Catalog. The catalogs may be viewed at <http://www.firstrespondertraining.gov>. A listing of courses that are currently approved for PSGP funding is included in the table below.

Funding for training courses not listed in Table 3 may be permitted on a case-by-case basis depending on the specific maritime security risk mitigation training needs of the eligible PSGP applicant. In such cases, an applicant will be required to explain in the IJ why none of the approved courses referenced in Table 3 satisfy the identified training need and must submit detailed course information for review and consideration by the local COTP field review team and the Nation Review Panel.

Table 3: Approved PSGP Training Courses

National Training and Education Division	
Course Number	Course Name
AWR-144	Port and Vessel Security for Public Safety and Maritime Personnel
AWR-213	Critical Infrastructure Security and Resilience Awareness
AWR-366-W	Developing a Cyber Security Annex for Incident Response
MGT-335	Event Security Planning for Public Professionals
MGT-335-W	Event Security Planning for Public Professionals, Web Based
MGT-400	Master of Arts Degree in Homeland Security
MGT-425	Homeland Security Executive Leaders Program (ELP)
MGT-452	Physical and Cybersecurity for Critical Infrastructure

MGT-456	Integration of Cybersecurity Personnel into the Emergency Management Operations Center for Cyber Incidents
PER-330	The Surface Transportation Emergency Preparedness and Security for Mass Transit and Passenger Rail (STEPS-PT)
PER-331	Surface Transportation Emergency Preparedness and Security for Senior Officials or Administrators (STEPS Sr)
Federal-Sponsored	
Course Number	Course Name
DHS-006-PREV	Seaport Security Anti-Terrorism Training Program (SSATP)
DHS-011-PREV	Maritime PRND Operations Course
DHS-016-PREV	Protective Measures Training for Security Officers, Mid-Level Safety/Security Supervisors, and Property Managers
DHS-011-PROT	NASBLA BOAT Tactical Operators Course
DHS-009-PROT	Boat Operator's Anti-Terrorism Training
DHS-126-RESP	NASBLA BOAT Crew Member Course
DHS-128-RESP	NASBLA - Pursuit and Stop Course
State-Sponsored	
Course Number	Course Name
CA-006-PREV	Maritime Company, Vessel, and Facility Security Officer
CA-007-PREV	Basic Maritime Security Awareness
CA-008-PREV	Basic First Responder Operational Maritime Security (FROMS)
CA-015-RESP	Maritime Facility Security Officer
CA-020-RESP	WMD & Terrorism Awareness for Security Professionals
ME-001-PROT	Maritime Security Awareness for Military, First Responder and Law Enforcement Personnel
ME-002-PROT	Command Strategies and Tactics for Marine Emergencies
ME-003-PROT	Tactical Boat Operations for Maritime Security and LE Personnel
ME-002-RESP	Emergency Medical Operations in the Maritime Domain
NJ-003-PREV	Government Agency Maritime Security Awareness Program (GAMSAP)
NJ-015-PREV	Security Awareness & Vigilance for Everyone
NY-001-PREV	Maritime Infrastructure Protection
NY-001-PROT	Safe Boat Operators
NY-002-PREV	Tactical Escorts and Security Zones
NY-002-PROT	Pattern Line Search/Recovery Course
NY-004-RESP	Vehicle Borne Improvised Explosive Device Security Checkpoint

Exercises

Exercise activities address the Soft Targets/Crowded Places; Cybersecurity; Emergent Threats; and Exercises Priorities.

Maritime entity training needs and qualification requirements of incident response personnel should be regularly tested through emergency exercises and drills. Exercises must test operational protocols that would be implemented in the event of a terrorist attack in the maritime environment in accordance with the Area Maritime Security Training Exercise Program (AMSTEP) or the Transportation Security Administration (TSA) Intermodal Security Training Exercise Program (I-STEP) guidelines. AMSTEP or I-STEP exercises will follow the latest change in requirements contained in the Navigation and Inspection Circular (NVIC) 09-02. Exercises must be designed, developed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP) located at <https://www.fema.gov/exercise>. Funding used for exercises will only be permitted for those exercises that are in direct support of a MTSA-regulated facility or a port area's MTSA-required exercises (*see* 33 C.F.R. § 105.220 for a facility and 33 C.F.R. § 103.515 for the AMSP). These exercises must be coordinated with the COTP and AMSC

and be consistent with HSEEP. More information on HSEEP may be found at <https://www.fema.gov/hseep>.

Recipients are required to submit an After Action Report/Improvement Plan (AAR/IP) for each PSGP-funded exercise to hseep@fema.dhs.gov, and the appropriate local COTP no later than 90 days after completion of the exercise conducted within the PSGP POP. Recipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. Recipients are required to use the HSEEP AAR/IP template located at <https://www.fema.gov/exercise>. PSGP funds may be used for the following exercise activities:

Funds Used to Design, Develop, Conduct, and Evaluate an Exercise. This includes costs related to planning, meeting space, and other meeting costs, facilitation costs, materials and supplies, travel, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low-risk setting. Any shortcoming or gap identified, including those for children and individuals with disabilities or access and functional needs, should be identified in an effective corrective action program that includes development of improvement plans that are dynamic documents, with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

Hiring of Full- or Part-Time Staff or Contractors/Consultants. Full- or part-time staff may be hired to support exercise-related activities. Such costs must be included within the funding allowed for program management personnel expenses, which must not exceed 10% of the total allocation. Dual compensation is never allowable, meaning, in other words, that an employee of a unit of government may not receive compensation from his or her unit or agency of government and from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both entities. Personnel hiring, overtime, and backfill expenses are permitted under this grant only to the extent that such expenses are for the allowable activities within the scope of the grant.

Overtime and Backfill Costs. The entire amount of overtime costs, including payments related to backfilling personnel that are the direct result of time spent on the design, development and conduct of exercises are allowable expenses. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or the awarding agency, whichever is more restrictive. Dual compensation is never allowable.

Travel. Domestic travel costs are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of exercise project(s). International travel costs are not permitted.

Supplies. Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise project(s) (e.g., gloves, non-sterile masks, and disposable protective equipment).

Other Items. These costs include the rental of space/locations for exercise planning and executing, rental of equipment, etc. Recipients are encouraged to use free public space, locations, or facilities, whenever available, prior to the rental of space, locations, or facilities. These also include costs that may be associated with inclusive practices and the provision of reasonable accommodations and modifications to provide full access for children and adults with disabilities.

The National Exercise Program (NEP) serves as the principal exercise mechanism for examining national preparedness and measuring readiness. Recipients are strongly encouraged to nominate exercises into the NEP. For additional information on the NEP, please refer to <http://www.fema.gov/national-exercise-program>.

Management and Administration

Management and administration (M&A) costs are allowed under this program. M&A costs are activities directly related to managing and administering the award. Recipients may use up to 5% of the amount of the award for their M&A and subrecipients may use up to 5% for M&A of the amount they receive.

PSGP funds may be used for the following M&A costs:

- Hiring full-time or part-time staff, including contractors and consultants, to execute the following:
 - Management of the awarded fiscal year's PSGP award;
 - Design and implementation of the awarded fiscal year's PSGP submission meeting compliance with reporting/data collection requirements, including data calls;
 - Information collection and processing necessary to respond to DHS/FEMA data calls;
 - Travel expenses related to PSGP grant administration; and
 - Acquisition of authorized office equipment, including personal computers or laptops for PSGP M&A purposes.

Allowable Indirect Costs

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal

Unallowable Costs

Projects that do not provide a compelling maritime security benefit or have a direct nexus toward maritime security risk mitigation are not permitted. For example, projects that are primarily for economic or safety benefit (as opposed to having a direct maritime security risk mitigation benefit) are ineligible for PSGP funding. In addition, projects that provide a broad homeland security benefit (e.g., a communication system or fusion center for an entire city, county, state, etc.) as opposed to providing primary benefit to the port are ineligible for PSGP funding since these projects should be eligible for funding through other preparedness grant programs. The following projects and costs are considered ineligible for award consideration:

- Grant funds must comply with [IB 426](#) and may not be used for the purchase of the following equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed;
- Projects in which federal agencies are the primary beneficiary or that enhance federal property, including sub-components of a federal agency;
- Projects that study technology development for security of national or international cargo supply chains (e.g., e-seals, smart containers, container tracking or container intrusion detection devices);
- Proof-of-concept projects;
- Development of training;
- Projects that duplicate capabilities being provided by the Federal Government (e.g., vessel traffic systems);
- Business operating expenses (certain security-related operational and maintenance costs are allowable—*see* “Maintenance and Sustainment” and “Operational Costs” for further guidance);

- Transportation Worker Identification Credential (TWIC) card fees;
- Reimbursement of pre-award security expenses;
- Outfitting facilities, vessels, or other structures with equipment or items providing a benefit rather than a direct security benefit. Examples of such equipment or items include, but are not limited to: office furniture, CD players, DVD players, AM/FM radios, TVs, stereos, entertainment satellite systems, entertainment cable systems and other such entertainment media, unless sufficient justification is provided. This includes weapons and associated equipment (i.e., holsters, optical sights, and scopes), including but not limited to, non-lethal or less-than-lethal weaponry including firearms, ammunition, and weapons affixed to facilities, vessels, or other structures;
- Expenditures for items such as general-use software, general-use computers, and related equipment (other than for allowable M&A activities, or otherwise associated) preparedness or response functions), general-use vehicles and licensing fees;
- Land acquisitions and right of way purchases;
- Funding for standard operations vehicles utilized for routine duties, such as patrol cars and fire trucks;
- Fuel costs (except as permitted for training and exercises);
- Exercise(s) that do not support maritime security preparedness efforts;
- Patrol vehicles and firefighting apparatus, other than those CBRNE detection equipped vehicles for port area and/or facility patrol or response purposes;
- Specialty vehicles such as trucks for towing boat trailers and armored personnel carriers;
- Providing protection training to public police agencies or private security services to support protecting VIPs or dignitaries;
- Aircraft pilot training, including aircraft operations such as aircraft ditch training;
- Post incident investigation training;
- Basic or advanced dive training (except marine unit CBRNE detection/response dive training);
- Training for personnel not primarily assigned to maritime security activities or MTSA required security personnel (e.g., vessel patrol officers, facility security officers); and
- Reimbursement for the maintenance and wear and tear costs of general use vehicles (e.g., construction vehicles) and emergency response apparatus (e.g., fire trucks, ambulances, repair or cleaning of Personal Protective Equipment (PPE), etc.).

Maintenance and Sustainment Costs

Maintenance and sustainment do not include general or routine operational maintenance activities that are inherently the responsibility of equipment owners. Eligible maintenance and sustainment costs are limited to:

- Maintenance or service plans provided by vendors at the time of purchase (contract only)
- Warranties provided at the time of purchase (contract only)
- Cost of specified repairs including parts and labor (contracted or in-house)
- Cost of specified replacement equipment and installation including parts and labor (contracted or in-house)

Ineligible maintenance and sustainment costs include:

- Supplies and labor for cleaning equipment (i.e., washing vessels)
- Equipment inspection (i.e., routine preventative maintenance checks)
- Pre-departure safety inspection

- General preventative maintenance service and trouble-shooting (e.g., recommended by manufacturer, such as belt, fluid, or oil changes) other than as provided through initial equipment purchase contract services, as explained above

Port-Wide Risk Management Plans

Port areas with existing Portside Risk Management 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/Resumption of Trade Plan (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.

Additional Port Security Resources

- U.S. Department of Transportation "BUILD" grants for National Infrastructure Investments may include funding to support roads, bridges, transit, rail, ports or intermodal transportation, see <https://www.transportation.gov/BUILDgrants>
- Cybersecurity assessments may be available via DHS CISA, see <https://www.dhs.gov/cisa/cybersecurity-assessments>

Sample Memorandum of Understanding/Agreement

The sample MOU/MOA below demonstrates all of the elements required in the PSGP NOFO for acceptance for review as part of a grant application from a state or local agency providing security services to MTSA-regulated entities.

**Memorandum of [Understanding / Agreement]
Between [provider of layered security] and [recipient of layered security]
Regarding [provider of layered security's] Use of Port Security Grant Program Funds**

1. **PARTIES.** The parties to this Agreement are the [Provider of Layered Security] and the [Recipient of security service].
2. **AUTHORITY.** This Agreement is authorized under the provisions of [applicable Area Maritime Security Committee (AMSC) authorities and/or other authorities].
3. **PURPOSE.** The purpose of this Agreement is to set forth terms by which [Provider of security service] shall expend Port Security Grant Program project funding in providing security service to [Recipient of security service]. Under requested PSGP grant, the [Provider of security service] must provide layered security to [Recipient of security service] consistent with the approach described in an approved grant application.
4. **RESPONSIBILITIES:** The security roles and responsibilities of each party are understood as follows:
 - (1) [Recipient of security service]
Roles and responsibilities in providing its own security at each MARSEC level
 - (2) [Provider of security service]
 - [-An acknowledgement by the facility that the applicant is part of their facility security plan.]
 - [-The nature of the security that the applicant agrees to supply to the regulated facility (waterside surveillance, increased screening, etc.).]
 - [-Roles and responsibilities in providing security to [Recipient of security service] at each MARSEC level.]
5. **POINTS OF CONTACT.** [Identify the POCs for all applicable organizations under the Agreement; including addresses and phone numbers (fax number, e-mail, or internet addresses can also be included).]
6. **OTHER PROVISIONS.** Nothing in this Agreement is intended to conflict with current laws or regulations of [applicable State] or [applicable local Government]. If a term of this agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.
7. **EFFECTIVE DATE.** The terms of this agreement will become effective on [EFFECTIVE DATE].
8. **MODIFICATION.** This agreement may be modified upon the mutual written consent of the parties.
9. **TERMINATION.** The terms of this agreement, as modified with the consent of both parties, will remain in effect until the grant end dates for an approved grant. Either party upon [NUMBER] day's written notice to the other party may terminate this agreement.

APPROVED BY: Organization and Title

Program Appendix H: Emergency Management Performance Grant Program

Alignment of EMPG to the National Preparedness System

EMPG contributes to the implementation of the National Preparedness System by supporting the building, sustainment, and delivery of core capabilities. Core capabilities are essential for the execution of critical tasks for each of the five mission areas outlined in the Goal. EMPG'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. DHS/FEMA requires recipients to prioritize grant funding to demonstrate how investments support closing capability gaps or sustaining capabilities identified in the THIRA/SPR process.

Emphasis is placed on capabilities that address the greatest risks to the security and resilience of the United States and the greatest risks along the Nation's borders. 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 Emergency Management Assistance Compact (EMAC). EMPG 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.

Reporting on the Implementation of the National Preparedness System

Identifying and Assessing Risk and Estimating Capability Requirements

By December 31, 2020, recipients are required to complete a THIRA/SPR that addresses all 32 core capabilities and is compliant with Comprehensive Preparedness Guide (CPG) 201, Third Edition. Specific guidance on the requirements for each core capability will be forthcoming in 2020, as some core capabilities have fewer reporting requirements than others. Beginning in 2020, recipients will also be required to respond to a series of planning-related questions as part of the THIRA/SPR.

Recipients are required to submit a THIRA every three (3) years to establish a consistent baseline for assessment. While the THIRA will be only required every three years, recipients will continue to be required to submit an SPR annually. For additional guidance on the THIRA/SPR, please refer to [Comprehensive Preparedness Guide \(CPG\) 201, Third Edition](#).

Reporting:

- In each EMPG recipient's Biannual Strategy Implementation Report ([BSIR](#)), as part of programmatic monitoring, the recipient should describe how expenditures support closing capability gaps or sustaining capabilities identified in the THIRA/SPR process. EMPG recipients will, on a project-by-project basis, check one of the following:
 - Building a capability with EMPG funding; or
 - Sustaining a capability with EMPG funding.

Building and Sustaining Core Capabilities

EMPG projects should describe how the proposed investment supports closing capability gaps or sustaining capabilities identified in the THIRA/SPR process.

NIMS Implementation

EMPG recipients are required to implement NIMS. EMPG funds may be used to meet the requirements described in the NIMS Implementation Objectives (<https://www.fema.gov/implementation-guidance-and-reporting>). 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, and response, mitigation, and recovery. EMPG 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 on NIMS implementation through the Unified Reporting Tool ([URT](#)).

Logistics Planning

Continuing the requirement from 2019, EMPG recipients are required to develop and maintain a Distribution Management (DM) plan as an annex to their existing Emergency Operations Plan (EOP). The DM plan should be updated by recipients on an annual basis. A question in the URT under the CPG 101 assessment is added to understand if a jurisdiction has developed and incorporated a DM plan in its 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 the following:
 - Requirements Defining
 - Resource Ordering
 - Distribution Methods
 - Inventory Management
 - Staging areas
 - Transportation
 - Demobilization

FEMA Regional Logistics Branch will work with EMPG recipients to provide technical assistance during the development and maintenance of their DM plans, and to ensure all recipients have effective distribution management plans capable of integrating with federal, nongovernmental organizations, private sector, and state, local, tribal and territorial stakeholders during major disasters.

Logistics Planning Resources

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

- **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.
- **Points of Distribution (PODs) Training:** FEMA Logistics developed a comprehensive POD training to assist states in developing actionable plans for emergency distribution and understanding associated challenges. Additional information, including an explanatory DVD, POD guide, and online exam, are available on the Emergency Management Institute's (EMI) website at <https://training.fema.gov/is/courseoverview.aspx?code=IS-26>.
- **Interagency Logistics (IL) Training:** This basic IL training course 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 the course by visiting: <https://training.fema.gov/emigrams/2018/1439%20-%20training%20opportunity%20-%2018540%20basic%20interagency%20logistics%20fy19.pdf?d=10/2/2018>.
- **Using Comprehensive Preparedness Guide (CPG) for Logistics Planning:** Recipients may find additional guidance in CPG 101 v2 on how to incorporate logistics into EOPs at <https://www.fema.gov/media-library/assets/documents/25975>.
- **Funding for Critical Emergency Supplies:** Critical emergency supplies—such as shelf stable products, water, and basic medical supplies—are an allowable expense under EMPG. Each state must have DHS/FEMA's approval of a five-year viable inventory management plan prior to allocating grant funds for stockpiling purposes. The inventory management five-year plan should include a distribution strategy and related sustainment costs if the grant expenditure is over \$100,000.

Reporting

EMPG recipients will submit their DM plan annex to FEMA Regional Logistics Staff for review on an annual basis. FEMA Regional Logistics Staff will review and rate the plans.

Evacuation Planning

EMPG recipients should review and update their EOP at least once every two years in accordance with Comprehensive Preparedness Guide (CPG) 101 v2, *Developing and Maintaining Emergency Operations Plans*. Recipients are highly 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 Mass Evacuation Incident Annex's planning considerations, and other FEMA documents related to evacuation planning, when developing their own Evacuation Plan or Annex. [National Response Framework](#) (NRF), Third Edition (June 2016); [NRF Mass Evacuation Incident Annex](#) (June 2008). Additional National Preparedness resources are available at <https://www.fema.gov/national-preparedness-resource-library>.

Disaster Housing Planning

Based on lessons learned from recent disasters, FEMA strongly encourages EMPG 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.

State-Led Disaster Housing Task Force

EMPG recipients are strongly encouraged to update their State Housing Strategy using the *State Housing Strategy Template* provided by FEMA Individual Assistance (IA) as part of their EOP or as a standalone document. In addition to the State Housing Strategy Template, recipients are encouraged to define and emphasize sheltering, short term, and permanent housing planning.

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. SLDHTFs 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:

- Complete the State Housing Strategy Template; and
- Establish a State Disaster Recovery Coordinator

State Housing Strategy Template

The State Housing Strategy Template, developed by FEMA IA, helps states identify priorities and document critical, jurisdiction-specific processes and procedures to promote an efficient disaster housing mission. The template walks recipients through the following planning considerations as seen in the table below:

Table 4: State Housing Template Sections and Planning Considerations

Template Section	Planning Considerations
SLDHTF Plan Organization	Participant inclusion, approaches for various types of housing disasters, available materials, available assistance programs, and sources for surge staffing
Housing Background	Identifying a jurisdictions current housing situation, priorities, capabilities, challenges, and known risks
Sheltering Phase Strategy	Identifying planning leads, current resources, timeline, key partners, cross-jurisdictional agreements, and other risks
Interim Housing Strategy	Identifying planning leads, current resources and capabilities, known areas of difficulty, key partners, relocation strategies, and risks
Permanent Housing Strategy	Identifying planning leads, long-term housing needs and prioritizations, current resources and capabilities, known areas of implementation challenges, relocation strategies, and risks
Pre-Disaster Activities	Creating communication plans, survivor transition plans, mitigation plans, and program closeout goals
Post-Disaster Activities	Prioritizing disaster housing recovery activities, creating timelines for project completion, documenting planned actions for assessing the availability of affordable housing resources and expediting the delivery of housing by expediting permitting and waiver processes, establishing an information sharing method,

Template Section	Planning Considerations
	creating an environmental and historical preservation strategy, identifying potential locations for Manufactured Housing Units and Recreational Vehicles, and identifying available federal disaster housing assistance

State-Administered Direct Housing Implementation

FEMA encourages states to develop the capacity to administer FEMA Direct Housing Assistance through a reimbursable Inter-Governmental Service Agreement (IGSA). Under this arrangement, FEMA determines disaster survivors’ eligibility for specific direct housing options and makes all determinations regarding continuing eligibility, appeals, and eligibility terminations. FEMA also monitors the state’s administration of approved Direct Housing Options to ensure compliance with federal environmental, historic preservation, and floodplain management requirements as well as program conditions specified within the IGSA. States that choose to administer Direct Housing Assistance through an IGSA are required to develop a Direct Housing Administrative Plan and are encouraged to establish pre-placed contract to support the delivery of direct housing. For more information, regarding Direct Housing Assistance, please visit Chapter 5 of the [Individuals and Households Unified Guidance](#).

Disaster Housing Exercises

Recipients 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 issues or administer FEMA Direct Housing Assistance under an IGSA
- 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

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 recipients include pre-disaster recovery planning as part of their State Readiness and Preparedness efforts by establishing a State Disaster Recovery Coordinator (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 technical assistance, to disaster-impacted communities.
- Enable State leadership to better organize and identify gaps in the state’s recovery capabilities.

Disaster Financial Management Policies and Procedures

Recent experience from the 2017 hurricane season and wildfires demonstrated the need for impacted jurisdictions to be able to immediately begin tracking and accounting 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.

State Administrative Plan

FEMA strongly recommends that EMPG 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. Table 5 details the processes that should be included in the State Administrative Plan and recommendations on where they should be placed:

Table 5: State Administrative Plan Guidance

State Administrative Plan Section Recommendations	Processes
<ul style="list-style-type: none"> • Section V Part D: Project Funding and Reimbursement • Section V Part G: Records and Reports 	<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Section V Part D: Project Funding and Reimbursement • Section V Part G: Records and Reports 	<ul style="list-style-type: none"> • A process to document disaster cost operations such as labor, equipment, and materials that are allowable under federal requirements
<ul style="list-style-type: none"> • Section V Part D: Project Funding and Reimbursement 	<ul style="list-style-type: none"> • A process to ensure that subrecipients are not receiving a duplication in benefits
<ul style="list-style-type: none"> • Section IV Part B: Organization and Staffing 	<ul style="list-style-type: none"> • A process to ensure pre-disaster contracts and procurement strategies are in place, if necessary

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

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 own Administrative Plan. The template can be found at <https://www.fema.gov/media-library/assets/documents/31208>.
- **Public Assistance Program and Policy Guide:** The Public Assistance Program and Policy Guide (PAPPG) combines all PA policy into a single volume and provides an overview of the PA program implementation process. The guide can be found at <https://www.fema.gov/media-library/assets/documents/111781>.
- **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 <https://www.fema.gov/public-assistance-frequently-asked-questions>.
- **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. The report can be found at <https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-120-D-Sep17.pdf>.

Validating Capabilities

All recipients will develop and maintain a progressive exercise program consistent with Homeland Security Exercise and Evaluation Program (HSEEP) guidance in support of the National Exercise Program (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.

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 Training and Exercise Plan (TEP) or an Integrated Preparedness Plan (IPP). Information related to TEPs and Training and Exercise Planning Workshops (TEPWs), as well as information about IPPs and Integrated Preparedness Planning Workshops (IPPWs), can be found on the HSEEP website at <https://www.fema.gov/HSEEP> and <https://preptoolkit.fema.gov/>.

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 at: <https://www.fema.gov/national-exercise-program> or reach out to the National Exercise Program directly at NEP@fema.dhs.gov.

Reporting

- Recipients must have a current multi-year TEP or IPP that identifies preparedness priorities and activities. The current multi-year TEP or IPP must be submitted to hseep@fema.dhs.gov before January 31 of each year.
 - Recipients are encouraged to enter their exercise information into the Preparedness Toolkit at <https://preptoolkit.fema.gov/>.
- Recipients must submit After-Action Report (AAR)/Improvement Plans (IPs) to hseep@fema.dhs.gov and indicate which fiscal year's funds were used (if applicable).
- Submission of AAR/IPs must be no later than December 31 of each year. Recipients are encouraged to submit AAR/IPs within 90 days after completion of the single exercise or progressive series.
 - Recipients are encouraged to submit AAR/IPs reflecting table top exercises which validate critical plans or those reflecting large-scale functional or full-scale exercises which took place at the state, territorial, tribal, or UASI level. Recipients are discouraged from submitting AAR/IPs specific to local jurisdictions which reflect drills.
 - If a recipient endures a significant real-world incident during the calendar year, they can submit the AAR from that event in place of one or more of the exercise AARs depending on the size and scale of the incident. Jurisdictions submitting real world AARs should include a request to do so with the AAR submission to hseep@fema.dhs.gov.
 - Recipients can access a sample AAR/IP template at <https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning>.

In addition to training activities aligned to and addressed in the TEP, all EMPG-funded personnel shall complete *either* the Independent Study courses identified in the Professional Development Series *or* the National Emergency Management Basic Academy delivered either by the Emergency Management Institute (EMI) or at a sponsored state, local, tribal, territorial, regional or other designated location. Further information on the National Emergency Management Basic Academy and the Emergency Management Professional Program can be found at: <https://training.fema.gov/empp/>. Previous versions of the IS courses meet the NIMS training requirement. A complete list of Independent Study Program Courses may be found at <http://training.fema.gov/is>. In addition to training activities aligned to and addressed in the TEP, all EMPG-funded personnel (including full- and part-time state, local, tribal and territorial (SLTT) recipients and subrecipients) shall 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), AND
- (2) Professional Development Series (PDS) OR the Emergency Management Professionals Program (EMPP) Basic Academy listed in the chart below.

*Note: NIMS training courses IS-100, IS-200, IS-700, and IS-800 only have to be taken once to fulfill requirements. Proof of completion of training requirements should be maintained by recipients so it can be produced when requested by DHS/FEMA during periodic reviews.

Exercise Requirements

While there are no minimum exercise requirements, FEMA Regional Administrators and State Emergency Management Directors will negotiate an exercise program that addresses capability gaps in the priority areas of logistics distribution management planning, evacuation plan/annex, disaster financial management, and catastrophic disaster housing. It is also recommended that all exercise projects describe

how they align to the Principals' Strategic Priorities: Operational Coordination and Communications, Cybersecurity, Stabilization and Restoration of Critical Lifelines, National Security Emergencies, Public Health Emergencies, Community Recovery and Economic Resilience, Mass Care and Housing, Continuity, and School Safety and Security. These exercises will be included in the EMPG work plan submitted for regional approval and the State's Training and Exercise Plan.

Reporting

- Recipients are required to develop a Multi-Year TEP that identifies a combination of exercises and associated training requirements that address priorities identified in the TEPW and builds from training gaps identified in the THIRA/SPR process. The TEP shall be submitted to hseep@fema.dhs.gov and the appropriate Regional EMPG manager, 90 days after the completion of the TEPW. Recipients are encouraged to enter their exercise information in the Preparedness Toolkit at <https://preptoolkit.fema.gov/web/hseep-resources>.
- Recipients must provide a list of completed training courses and exercises and the Training and Exercise Data Table to be included in the Quarterly Performance Progress Report.
- Recipients must include the TEP percentage completion outlined in the EMPG Work Plan in the Quarterly Performance Progress Report.
- Recipients should submit their AAR/IP to the HSEEP inbox (HSEEP@fema.dhs.gov) and copy their assigned Regional EMPG manager. Submission of the AAR/IP shall be no later than 90 days after completion of the exercise. Recipients are encouraged to enter their AAR/IP in the Preparedness Toolkit at <https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning>. Recipients are reminded of the importance of implementing corrective actions iteratively throughout the exercise cycle. This link provides access to a sample AAR/IP template: <https://preptoolkit.fema.gov/web/hseep-resources/improvement-planning>.

If a state, territory, 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 FEMA Regional EMPG Manager through the Quarterly Performance Progress Report. Exemptions will be reviewed on a case-by-case basis by the Regional EMPG Manager.

Reviewing and Updating Planning Products

Based on the applicant's current THIRA/SPR, capability levels, resources, and 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.

Additional Considerations

Strengthening Governance Integration

DHS/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 that pose 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. Disparate governance structures 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 and inclusive governance systems better ensure that disparate funding streams are coordinated and applied for maximum impact.

DHS/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 as identified in the SPR 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 DHS/FEMA grants support, must include local government representatives. At the state and regional levels, local risk assessments must be included in the overarching analysis to ensure that all threats and hazards are accounted for.
- **Accountability:** DHS/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-state partnerships and dependencies at the state and regional levels, including those within metropolitan areas, must be recognized.

Program Performance Reporting Requirements

Performance Progress Reports (PPR)

Specific to EMPG, recipients are responsible for providing updated performance reports to FEMA using a Microsoft Word (Word) document summary attached in ND Grants on a quarterly basis. As explained in the *Standardized Programmatic Reporting* section below, the Quarterly Performance Progress Reports must be based on the approved EMPG Work Plan and are due no later than 30 days after the end of the quarter (i.e., on January 30, April 30, July 30, and October 30). Recipients must complete the summary of activities and submit it as an attachment to the ND Grants system.

Recipients are required to report quarterly on progress toward completing activities and projects approved in their EMPG Work Plans, how expenditures support maintenance and sustainment of core capabilities, and progress made toward implementing the National Preparedness System. This includes reporting on the following information:

- List of completed training courses and exercises and the Training and Exercise Data Table
- Percent completion of the TEP outlined in the EMPG Work Plan

Programmatic Reporting Periods and Due Dates

The following reporting periods and due dates apply for the PPR:

Reporting Period	Report Due Date
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30

Standardized Programmatic Reporting for EMPG

The EMPG Work Plan Template was modified to standardize data collection for improved analysis and reporting. The EMPG Work Plan includes five components: (1) Program and Budget Narrative, (2) Personnel Data Table, (3) Training Data Table, (4) Exercise Data Table, and (5) Grant Activities Outline. Baseline data on personnel, training, and exercises, as well as the Grant Activities Outline, must be provided in the EMPG Work Plan at the time of application and will form the basis of the Quarterly Performance Progress Report Word document submissions. The Grant Activities Outline is structured to enable reporting of quarterly activities according to Emergency Management Function (EMF) projects, as well as standardized reporting of activity completion status. The EMPG Work Plan must summarize program activities in the following areas:

- **Planning:** Planning efforts should span all five Goal mission areas. The EMPG Work Plan should provide a baseline for determining potential threats and hazards, required capabilities, and required resources. It should also establish a framework for roles and responsibilities. Planning efforts should demonstrate whole community engagement to create a strategic, operational, and/or community-based approach to preparedness.
- **Organization:** EMPG funds may be used for all-hazards emergency management operations, staffing, and other day-to-day activities in support of emergency management, including staffing the State Hazard Mitigation Officer (SHMO) position, as well as Community Emergency Response Team (CERT) and Citizen Corps positions at the state and local levels in order to promote whole community engagement in all phases of emergency management and across the mission areas.
- **Equipment:** Allowable EMPG equipment categories are listed on the web-based version of the Authorized Equipment List (AEL), which is available at <https://www.fema.gov/authorized-equipment-list>. Unless otherwise stated, equipment must meet all mandatory regulatory and/or DHS/FEMA-adopted standards to be eligible for purchase using these funds. In addition, agencies will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.
- **Training:** EMPG funds may be used for a range of emergency management-related training activities to enhance the capabilities of state and local emergency management personnel, including establishing, supporting, conducting, and attending training deliveries. Training activities should align to a current, Multi-Year TEP developed through an annual Training and Exercise Plan Workshop (TEPW) and should reflect efforts to address training capabilities gaps identified through the THIRA/SPR processes.
- **Exercises:** Exercises conducted with grant funds should test and evaluate performance towards meeting capability targets established in a jurisdiction's THIRA for the core capabilities needed to address its greatest risks. Exercise priorities should align to a current, Multi-Year TEP developed through an annual TEPW.

EMPG Funding Guidelines

Allowable Costs

Management and Administration (M&A)

M&A activities are those defined as directly relating to the management and administration of EMPG funds, such as financial management and monitoring. It should be noted that salaries of state and local emergency managers are not typically categorized as M&A, unless the state or local EMA chooses to assign personnel to specific M&A activities.

If the SAA is not the EMA, the SAA is not eligible to retain funds for M&A. M&A costs are allowable for both state and local-level EMAs. The state EMA may use up to 5% of the EMPG award for M&A purposes. In addition, local EMAs may retain and use up to 5% of the amount received from the state for local M&A purposes.

Indirect Costs

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal.

Whole Community Preparedness

EMPG funds may be used to foster whole community preparedness for disasters and emergencies as stated in [FEMA Strategic Plan](#), particularly Part 1.3. Recipients, and DHS/FEMA must learn from and work with a broad and inclusive base of stakeholders to understand the circumstances and challenges different groups of people face, particularly those who may have the hardest time in the aftermath of a disaster, such as the aging population and those with access and functional needs. By engaging these stakeholders, EMPG recipients can help DHS/FEMA develop and promote a suite of well-targeted solutions for individuals and communities to adopt. Recipients should coordinate preparedness initiatives with DHS/FEMA and whole community partners to efficiently apply federal funding to reach the goal of individual and community resilience.

Planning

Planning spans all five National Preparedness Goal (the Goal) mission areas and provides a methodical way to engage the whole community in the development of a strategic, operational, and/or community-based approach to preparedness. EMPG Program funds may be used to develop or enhance emergency management planning activities. Some examples include:

Emergency Operations Plan

- Maintaining a current EOP that is aligned with guidelines set out in CPG 101 v2 <https://www.fema.gov/media-library/assets/documents/25975>
- Modifying existing incident management and emergency operations plans
- Developing/enhancing large-scale and catastrophic event incident plans

Communications Plans

- Developing and updating Statewide Communication Interoperability Plans
- Developing and updating Tactical Interoperability Communications Plans

Administrative Plans

- Developing/enhancing financial and administrative procedures for use before, during, and after disaster events in support of a comprehensive emergency management program

Whole Community Engagement/Planning

- Developing or enhancing mutual aid agreements/compacts, including required membership in EMAC
- Developing/enhancing emergency operations plans to integrate citizen/volunteer and other non-governmental organization resources and participation
- Integrating program design and delivery practices that ensure representation and services for under-represented, diverse populations that may be more impacted by disasters, including children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity, and other underserved populations

Resource Management Planning

- Developing/enhancing logistics and resource management plans
- Developing/enhancing volunteer and/or donations management plans

Shelter and Evacuation Planning

- Developing/enhancing sheltering and evacuation plans, including plans for: alerts/warning, crisis communications, pre-positioning of equipment for areas potentially impacted by mass evacuations, and re-entry

Recovery Planning

- Disaster housing planning, such as creating/supporting a state disaster housing task force and developing/enhancing state disaster housing plans
- Pre-event response, recovery, and mitigation plans in coordination with state, local, and tribal governments
- Developing/enhancing other response and recovery plans
- Developing recovery plans and preparedness programs consistent with the principles and guidance in the National Disaster Recovery Framework (NDRF) that will provide the foundation for recovery programs and whole community partnerships. Preparedness and pre-disaster planning were given special attention within the NDRF with specific guidance: *Planning for a Successful Disaster Recovery* (pages 63-70). For more information on the NDRF see <http://www.fema.gov/pdf/recoveryframework/ndrf.pdf> and <http://www.fema.gov/media-library-data/1423604728233-1d76a43cabf1209678054c0828bbe8b8/EffectiveCoordinationofRecoveryResourcesGuide020515vFNL.pdf>

Continuity Planning

Continuity planning and operations are an inherent element of each core capability. Continuity operations increase resilience and the probability that organizations can perform essential functions. DHS/FEMA develops and promulgates Federal Continuity Directives (FCDs) to establish continuity program and planning requirements for executive departments and agencies and Continuity Guidance Circulars (CGCs) for SLTT governments, non-governmental organizations, and private sector critical infrastructure owners and operators. This direction and guidance assist in developing capabilities for continuing the essential functions of federal, state, local, tribal, territorial governmental entities as well as the public/private critical infrastructure owners, operators, and regulators enabling them.

Presidential Policy 40, FCD 1, FCD 2, CGC 1, and CGC 2 outline the overarching continuity requirements and guidance for organizations and provide guidance, methodology, and checklists. For additional information on continuity programs, guidance, and directives, visit <http://www.fema.gov/guidance-directives> and <https://www.fema.gov/national-continuity-programs>.

Allowable continuity planning activities include the development of the following:

- Continuity of operations (COOP) and Continuity of Government (COG) planning products for the continuance of essential functions and associated leadership;
- Risk-based needs assessments based on the THIRA to inform risk mitigation efforts to ensure the continuity of essential functions and associated leadership; and
- Public and private sector outreach and messaging regarding continuity resilience benefits and strategies.

Organization

Per the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, Pub. L. No. 93-288, as amended, (42 U.S.C. §§ 5121-5207), EMPG funds may be used for all-hazards emergency management operations, staffing, and other day-to-day activities in support of emergency management, including hazard mitigation staffing of the State Hazard Mitigation Officer (SHMO) position; staffing CERT and Citizen Corps positions at the state and local levels to promote whole community engagement in all phases of emergency management; performing closeout activities on FEMA Disaster Assistance grants; staffing permanent technical advisors on children's needs at the state, local, tribal, and territorial levels and supporting fusion center analysts who are directly involved in all-hazards preparedness activities as defined by the Stafford Act. Proposed staffing activities should be linked to accomplishing the activities outlined in the EMPG Work Plan. Recipients are encouraged to fund at least one dedicated Planner, Training Officer, and Exercise Officer. Personnel costs, including salary, overtime, compensatory time off, and associated fringe benefits, are allowable costs with EMPG funds. These costs must comply with 2 C.F.R. Part 200, Subpart E – Cost Principles.

Federal (and Mutual Aid) Emergency Response Official (F/ERO) Credentialing and Validation

The following costs related to F/ERO credentialing and validation are allowable under EMPG:

- Working group meetings and conferences relating to emergency responder credentialing and validation;
- Compiling data to enter into an emergency responder repository;
- Coordinating with other state, local, territorial, and tribal partners to ensure interoperability among existing and planned credentialing and validation systems and equipment; and

- Planning to incorporate emergency responder identity and credential validation into training and exercises.

Equipment

Allowable equipment categories for EMPG are listed on the web-based version of the Authorized Equipment List (AEL) at <https://www.fema.gov/authorized-equipment-list>. Unless otherwise stated, equipment must meet all mandatory regulatory and/or FEMA-adopted standards to be eligible for purchase using these funds. In addition, agencies will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Allowable equipment includes equipment from the following AEL categories:

- Personal Protective Equipment (PPE) (Category 1)
- Information Technology (Category 4)
- Cybersecurity Enhancement Equipment (Category 5)
- Interoperable Communications Equipment (Category 6)
- Detection Equipment (Category 7)
- Power Equipment (Category 10)
- Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Reference Materials (Category 11)
- CBRNE Incident Response Vehicles (Category 12)
- Physical Security Enhancement Equipment (Category 14)
- CBRNE Logistical Support Equipment (Category 19)
- Other Authorized Equipment (Category 21)

In addition to the above, general purpose vehicles may be procured in order to carry out the responsibilities of the EMPG. If recipients have questions concerning the eligibility of equipment not specifically addressed in the AEL, they should contact their Regional EMPG Manager for clarification. Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 C.F.R. Part 200, including 2 C.F.R. §§ 200.310, 200.313, and 200.316.

Requirements for Small Unmanned Aircraft System

All requests to purchase Small Unmanned Aircraft System (SUAS) must comply with [Information Bulletin \(IB\) 426](#) and must include the policies and procedures in place to safeguard individuals' privacy, civil rights, and civil liberties in the jurisdiction that will purchase, take title to, or otherwise use the SUAS equipment.

Funding for Critical Emergency Supplies

Critical emergency supplies—such as shelf stable products, water, and basic medical supplies—are an allowable expense under EMPG. DHS/FEMA must approve a state's five-year viable inventory management plan prior to allocating grant funds for stockpiling purposes. The five-year plan should include a distribution strategy and related sustainment costs if the grant expenditure is over \$100,000.

Training

EMPG funds may be used for a range of emergency management-related training activities to enhance the capabilities of state and local emergency management personnel through the establishment, support, conduct, and attendance of training. Training activities should align to a current, Multi-Year TEP developed through an annual TEPW and build from training gaps identified in the THIRA/SPR process. Further guidance concerning the TEP and the TEPW can be found at <https://pretoolkit.fema.gov/web/hseep-resources/home>.

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 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 <https://www.fema.gov/training-0>.

All EMPG-funded personnel are expected to be trained emergency managers. In addition to training activities aligned to and addressed in the TEP, all EMPG -funded personnel (including full- and part-time state, local, tribal, and territorial (SLTT) recipients and subrecipients) shall 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)⁴ AND
- 2) Professional Development Series (PDS) OR the Emergency Management Professionals Program (EMPP) Basic Academy listed in the chart below.

Professional Development Series or Basic Academy		
PDS Professional Development Series	Basic Academy Basic Academy Pre-requisites and Courses	
IS-120.a An Introduction to Exercises	OR	IS-100 (any version) Introduction to the Incident Command System
IS-230.d Fundamentals of Emergency Management		IS-700 (any version) National Incident Management System (NIMS)-An Introduction
IS-235.b Emergency Planning		IS-800 (any version) National Response Framework, An Introduction
IS-240.b Leadership and Influence		IS-230.d Fundamentals of Emergency Management
IS-241.b Decision Making and Problem Solving		E/L101 Foundations of Emergency Management

⁴ NIMS training courses IS-100, IS-200, IS-700, and IS-800 only have to be taken once to fulfill requirements.

Professional Development Series or Basic Academy	
PDS Professional Development Series	Basic Academy Basic Academy Pre-requisites and Courses
IS-242.b Effective Communication	E/L102 Science of Disasters
IS-244.b Developing and Managing Volunteers	E/L103 Planning Emergency Operations
	E/L104 Exercise Design
	E/L105 Public Information & Warning

Recipients must maintain proof of completion of training requirements.

EMPG funds may be used for emergency management-related training activities to enhance the capabilities of state and local emergency management personnel. Training activities should align to a current, Multi-Year TEP developed through an annual Training and Exercise Planning Workshop (TEPW) and build from training gaps identified in the THIRA/SPR process. Further guidance concerning the TEP and the TEPW can be found at <https://preptoolkit.fema.gov/web/hseep-resources/program-management>. Training should:

- Foster the development of a community-oriented approach to emergency management that emphasizes engagement at the community level;
- Strengthen best practices; and
- Provide a path toward building sustainable resilience.

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 a TEP is developed and implemented.

Additional Training Information

Per DHS/FEMA Grant Programs Directorate [Information Bulletin 432](#), Review and Approval Requirements for Training Courses Funded Through Preparedness Grants, issued on July 19, 2018, states, territories, tribal entities, and high-risk urban areas are no longer required to request approval from FEMA for personnel to attend non-DHS FEMA training as long as the training is coordinated with and approved by the state, territory, tribal, or high-risk urban area Training Point of Contact (TPOC) and falls within the FEMA mission scope and the jurisdiction’s Emergency Operations Plan (EOP). For additional information on review and approval requirements for training courses funded with preparedness grants, please refer to the following policy: <http://www.fema.gov/media-library/assets/documents/34856>.

DHS/FEMA will conduct periodic reviews of all state, territory, and urban area training funded by DHS/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.

For further information on developing courses using the instructional design methodology and tools that can facilitate the process, SAAs and TPOCs are encouraged to review the NTED Responder Training Development Center (RTDC) website at <https://www.firstrespondertraining.gov/trdc/state/>.

NTED's National Preparedness Course Catalog

This online searchable catalog features a compilation of courses managed by the three primary DHS/FEMA training organizations: the CDP, EMI, and NTED. The catalog features a wide range of course topics in multiple delivery modes DHS/FEMA for Federal, state, local, territorial, and tribal audiences. The catalog is located here: <http://www.firstrespondertraining.gov>.

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 EMPG intent and the course content is sound and current. While reporting training activities through Web Forms is not required under EMPG, the system remains available and can be accessed through the DHS/FEMA Toolkit located at <https://www.firstrespondertraining.gov/frt/> to support recipients in their own tracking of training deliveries. Additional types of training or training related activities include, but are not limited to, the following:

- Developing/enhancing systems to monitor training programs
- Conducting all hazards emergency management training
- Attending EMI training or delivering EMI train-the-trainer courses
- Attending other DHS/FEMA-approved emergency management training
- State-approved, locally-sponsored CERT training
- Mass evacuation training at local, state, territorial and tribal levels

Allowable training-related costs include the following:

- **Funds Used to Develop, Deliver, and Evaluate Training:** Includes costs related to administering training, such as planning, scheduling, facilities, materials and supplies, reproduction of materials, and equipment. Training should provide the opportunity to demonstrate and validate skills learned, as well as to identify any gaps in these skills. Any training or training gaps, including those for children and individuals with disabilities or access and functional needs, should be identified in the Multi-Year TEP and addressed in the training cycle. States are encouraged to use existing training rather than developing new courses. When developing new courses, states are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model for instruction design. <https://www.firstrespondertraining.gov>.
- **Overtime and Backfill:** Overtime costs, including payments related to backfilling personnel, that are the direct result of attendance at DHS/FEMA and/or approved training courses and programs are allowable. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or DHS/FEMA, whichever is applicable. In no case is dual compensation allowable. That is, an employee of a unit of government may not receive compensation from their unit or agency of government *and* from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though such work may benefit both activities.
- **Travel:** Travel costs (e.g., airfare, mileage, per diem, and hotel) are allowable as expenses by employees who are on travel status for official business related to approved training. International travel is not an allowable cost under this program unless approved in advance by FEMA.
- **Hiring of Full- or Part-Time Staff or Contractors/Consultants:** Full- or part-time staff or contractors/consultants may be hired to support direct training-related activities. Payment of salaries and fringe benefits must be in accordance with the policies of the state or unit(s) of local government and have the approval of the state or DHS/FEMA, whichever is applicable.

- **Certification/Recertification of Instructors:** Costs associated with the certification and recertification of instructors are allowed. States are encouraged to follow the FEMA Instructor Quality Assurance Program to ensure a minimum level of competency and corresponding levels of evaluation of student learning. This is particularly important for those courses which involve training of trainers.

Exercises

Allowable exercise-related costs include:

- **Funds Used to Design, Develop, Conduct and Evaluate Preparedness Exercises:** This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, travel, and documentation. Recipients are encouraged to use free public space/locations/facilities, whenever available, prior to the rental of space/locations/facilities. Exercises should provide the opportunity to demonstrate and validate skills learned, as well as to identify any gaps in these skills. Gaps identified during an exercise, including those for children and individuals with disabilities or access and functional needs, should be included in the After-Action Report (AAR)/Improvement Plan (IP) and addressed in the exercise cycle.
- **Hiring of Full- or Part-Time Staff or Contractors/Consultants:** Full- or part-time staff may be hired to support direct exercise activities. Payment of salaries and fringe benefits must be in accordance with the policies of the state or unit(s) of local government and have the approval of the state or DHS/FEMA, whichever is applicable. The services of contractors/consultants may also be procured to support the design, development, conduct, and evaluation of exercises.
- **Overtime and Backfill:** The entire amount of overtime costs, including payments related to backfilling personnel, that are the direct result of time spent on the design, development and conduct of exercises are allowable expenses. These costs are allowed only to the extent the payment for such services is in accordance with the policies of the state or unit(s) of local government and has the approval of the state or DHS/FEMA, whichever is applicable. Dual compensation is never allowable, meaning, in other words, that an employee of a unit of government may not receive compensation from their unit or agency of government *and* from an award for a single period of time (e.g., 1:00 p.m. to 5:00 p.m.), even though their work may benefit both entities.
- **Travel:** Travel costs (e.g., airfare, mileage, per diem, hotel) are allowable as expenses by employees who are on travel status for official business related to the planning and conduct of the exercise activities.
- **Supplies:** Supplies are items that are expended or consumed during the course of the planning and conduct of the exercise activities (e.g., gloves, non-sterile masks, and disposable protective equipment).
- **HSEEP Implementation:** This refers to costs related to developing and maintaining an exercise program consistent with HSEEP.
- **Other Items:** These costs are limited to items consumed in direct support of exercise activities, such as space/locations rentals for planning and conducting an exercise, equipment rentals, and the procurement of other essential nondurable goods. Costs associated with inclusive practices and the provision of reasonable accommodations and modifications that facilitate full access for children and adults with disabilities are allowable.

Unauthorized exercise-related costs include:

- Reimbursement for maintenance and/or wear and tear costs of general use vehicles (e.g., construction vehicles) and emergency response apparatus (e.g., fire trucks, ambulances). The only vehicle costs that are reimbursable are fuel/gasoline or mileage.
- Equipment that is purchased for permanent installation and/or use, beyond the scope of exercise conduct (e.g., electronic messaging signs)
- Durable and nondurable goods purchased for installation and/or use beyond the scope of exercise conduct

Construction and Renovation

Construction and renovation projects for a state, local, tribal, or territorial government's principal Emergency Operations Center (EOC), as defined by the SAA are allowable under the EMPG. DHS/FEMA must provide written approval prior to the use of any EMPG funds for construction or renovation. Requests for EMPG funds for construction of an EOC must be accompanied by an EOC Investment Justification (located in the Related Documents tab of the EMPG [grants.gov](#) posting) to their Regional EMPG Manager for review. Additionally, recipients are required to submit a SF-424C Form and Budget detail citing the project costs.

When applying for funds to construct communication towers, recipients and subrecipients must submit evidence that the Federal Communication Commission's (FCC's) Section 106 review process has been completed and submit all documentation resulting from that review to FEMA prior to submitting materials for EHP review. Recipients and subrecipients are also 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 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 EMPG Regional Program Manager within six months of the award, and completed EHP review materials must be submitted no later than 12 months before the end of the period of performance. EHP review packets should be sent to gpdehpinfo@fema.gov.

EMPG recipients using funds for construction projects must comply with the *Davis-Bacon Act* and subsequent legislation (40 U.S.C. §§ 3141 *et seq.*). 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. Additional information regarding compliance with the *Davis-Bacon Act*, including Department of Labor (DOL) wage determinations, is available from the following website: <https://www.dol.gov/whd/govcontracts/dbra.htm>.

Maintenance and Sustainment

Use of DHS/FEMA preparedness grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable under all active grant awards, unless otherwise noted.

EMPG 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 policy set forth in [IB 379: Guidance to State Administrative Agencies to](#)

[Expedite the Expenditure of Certain DHS/FEMA Grant Funding](#) allows for the expansion of eligible maintenance and sustainment costs, which 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) Shareable through the 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 DHS/FEMA preparedness grant program dollars. Additional guidance is provided in DHS/FEMA Policy FP 205-402-125-1, *Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants*, located at: <http://www.fema.gov/media-library/assets/documents/32474>.

Unallowable Costs

- Grant funds may not be used for:
 - Unallowable Equipment: Grant funds must comply with [IB 426](#) and may not be used for the purchase of the following equipment: firearms, ammunition, grenade launchers, bayonets, or weaponized aircraft, vessels, or vehicles of any kind with weapons installed.
 - Expenditures for weapons systems and ammunition
 - Costs to support hiring sworn public safety officers for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities
 - Activities and projects unrelated to the completion and implementation of the EMPG

Recipients should consult with their EMPG Regional Program Manager prior to making any investment that does not clearly meet the allowable expense criteria established in this NOFO.

EMPG Work Plan

EMPG Work Plan Instructions

All EMPG applicants are encouraged to use the templates to submit a required Work Plan that outlines the state's emergency management sustainment and enhancement efforts, including new and ongoing activities and projects, proposed for the EMPG period of performance. The Work Plan consists of a Program and Budget Narrative, Personnel Data Table, Training Data Table, Exercise Data Table, and Grant Activities Outline. EMPG Regional Program Managers will work closely with states to monitor Work Plans during the performance period and may request further documentation from the recipients to clarify the projected work plan. Prior to submission of the EMPG Work Plan, the applicant must work with the Regional Administrator or designated FEMA Regional Program Manager to ensure that regional or State priorities are properly addressed in the EMPG Work Plan. In addition, the EMPG Regional Administrator must approve final Work Plans before states may draw down EMPG funds. Grant funds will be released upon approval of the state's final Work Plan.

Program and Budget Narrative

Provide a brief description of the state emergency management priorities and initiatives that will be addressed with EMPG funds. In addition, the narrative should address the following:

- Overview of the state's risk profile resulting from the current THIRA
- Areas of need identified through assessment processes such as the SPR, Emergency Management Accreditation Program assessment process, National Emergency Communications Plan Goal Assessments, or other emergency management assessment processes
- Baseline inventory of where states are now, relative to goals and objectives identified in relevant strategic plans per CPG 101v2
- State emergency management priorities and planning focus for current budget year (including linkage to the core capabilities identified in the Goal)
- Detailed Budget Narrative justifying the requested funding for the identified Work Plan activities
- Detailed description of how projects and programmatic activities support the building or sustainment of the core capabilities as outlined in the Goal

Personnel Data Table

To facilitate consistent data reporting and performance measures collection, a Personnel Data Table should be completed for state, local, tribal, and territory personnel supported with EMPG funds. This will assist in documenting the extent to which EMPG funding supports personnel at the state level. Submit this template with the EMPG Work Plan and a roster of EMPG-funded personnel. The roster of EMPG-funded personnel should be updated only if numbers change more than 10% during the award period of performance.

Personnel Data Table Template

Personnel Metrics	Data
EMPG funds (federal and match) allocated towards state emergency management personnel	
EMPG funds (federal and match) allocated towards non-state emergency management personnel (local, tribal, territories)	
Total Number of state emergency management full-time equivalent (FTE) personnel (including those supported and not supported by EMPG)	
Number of state emergency management full-time equivalent (FTE) personnel supported (fully or partially) by EMPG	
Total number of state, local, tribal, and territory emergency management personnel supported (fully or partially) by EMPG	

Personnel Data Table Definitions

- Line 1 – All EMPG funds (federal and match) allocated for state emergency management personnel
- Line 2 – All EMPG funds (federal and match) allocated towards non-state emergency management personnel (local, tribal, territories)
- Line 3 – Total number of state emergency management full-time equivalent (FTE) personnel (including those supported and not supported by the EMPG)
- Line 4 – Number of state emergency management full-time equivalent (FTE) personnel supported by the EMPG
- Line 5 – Total number of state and local emergency management personnel funded (fully or partially) by the EMPG. This number provides the "Universe" number for the training and exercise templates

Training Data Table

To facilitate consistent data reporting and performance measures collection, a Training Data Table should be completed for training courses that meet the EMPG reporting requirements. This template should reflect training activities outlined in the Multi-Year TEP and completion of EMPG training requirements. EMPG-funded personnel should complete the listed training requirements and record proof of completion.

Training Data Table Template

Name of Training	EMPG Required Training? (Y/N)	Number of Personnel Trained	Total Number of SLTT EMPG Funded Personnel	Total Number of SLTT EMPG Funded Personnel that completed the Course	Training Identified in TEP (Y/N)

Training Data Table Definitions

- Column 1 – Name of training
- Column 2 – Is the course required of EMPG-funded personnel?
- Column 3 – Number of personnel trained
- Column 4 – Total number of SLTT EMPG-funded personnel (Universe)
- Column 5 – Total number of SLTT EMPG-funded personnel that completed the course
- Column 6 – Is the training identified in the Multi-Year TEP?

Exercise Data Table

To facilitate consistent data reporting and performance measure collection, an Exercise Data Table should be completed for any exercises that meet EMPG requirements and/or exercises conducted in whole or part with EMPG funds.

Exercise Data Table Template

Name/ Description of Exercise	Date Exercise Scheduled/Completed	Type of Exercise	Program Priority Exercised	Exercise Fulfills Progressive Exercise Requirement (Y/N)	Total # of SLTT EMPG Funded Personnel	Number of SLTT EMPG Program Funded Personnel Participating in Exercise	Exercise Fulfills EMPG Exercise Participation Requirement (Y/N)	Exercise Identified in TEP (Y/N)

Exercise Data Table Definitions:

- **Column 1** – Name/Description of exercise
- **Column 2** – Date of exercise
- **Column 3** – Type of exercise (e.g., seminar, workshop, tabletop, games, drills, functional, and/or full-scale)
- **Column 4** – Program priority associated with the exercise
- **Column 5** – Is the exercise part of a progressive exercise series?
- **Column 6** – Total number of SLTT EMPG Funded Personnel
- **Column 7** – Total number of SLTT EMPG Funded Personnel Participating in Exercise
- **Column 8** – Does the exercise fulfill the EMPG requirement that EMPG Program funded personnel participate in no less than three exercises?
- **Column 9** – Is exercise identified in the multi-year TEP?

Grant Activities Outline

To facilitate performance measures and focus on outcomes, an EMPG Grant Activities Outline should be completed for activities supported with EMPG funds (including construction and renovation projects). The data outlined in this template will be used to evaluate the timely completion of planned emergency management activities. Recipients are encouraged to complete a separate Grant Activities Outline for each Emergency Management Function (EMF). Quarterly training activities should be reported against EMF #13, “Training,” and quarterly exercise activities should be reported against EMF #14, “Exercises, Evaluations and Corrective Actions.” Recipients should complete a template as shown on the next page and address the following areas:

- **Name of Planned Project:** Provide a descriptive name of each planned project. Examples include “Development of Emergency Function Annexes”, “Development of Earthquake Scenario Loss Estimations”, “Implementation of Statewide Interoperability Plan”, “NIMS Training for Emergency Management Personnel”, “Development of Emergency Preparedness Plan for Individuals with Disabilities”, etc.
- **Project Objective:** Briefly explain the major objective of the project, including how the project will address gaps identified through various assessments conducted.
- **Core Capability Addressed:** Briefly describe which of the 32 core capabilities (multiple can be selected) the project addresses.
- **Performance Measure and Basis of Evaluation:** Indicate the performance measure that will be used to evaluate this project.
- **Challenges/Risks:** Identify any challenges to implementing this project or any of its activities.
- **Quarterly Activity:** Break each project down into quarterly activities. For each quarter, briefly identify the activities that will accomplish the planned project. This information will provide the foundation for the second component of the Quarterly Performance Progress Report.
- **Step:** Provide the status of planned quarterly activities (Initiate, Plan, Execute, Control, and Closeout).
- **Comments:** Briefly describe the reason for the project status and provide other comments as needed. Include the number of training sessions funded and the number of personnel trained in this section.

EMPG Grant Activities Outline - Template

Name of Planned Project:			
Project Objective:			
Core Capabilities Addressed:			
Performance Measure and Basis of Evaluation:			
Challenges/Risks:			
1st Quarter Activity	Planned Activities:	Step:	Comments:
2nd Quarter Activity	Planned Activities:	Step:	Comments:
3rd Quarter Activity	Planned Activities:	Step:	Comments:
4th Quarter Activity	Planned Activities:	Step:	Comments:
5th Quarter Activity	Planned Activities:	Step:	Comments:
6th Quarter Activity	Planned Activities:	Step:	Comments:
7th Quarter Activity	Planned Activities:	Step:	Comments:
8th Quarter Activity	Planned Activities:	Step:	Comments:

Project Management Lifecycle

Steps	Description	Process
Initiate	The authorization to begin work or resume work on any particular activity.	Involves preparing for, assembling resources and getting work started. May apply to any level, e.g. program, project, phase, activity, task.
Plan	The purposes of establishing, at an early date, the parameters of the project that is going to be worked on as well as to try to delineate any specifics and/or any peculiarities to the project as a whole and/or any specific phases of the project.	Involves working out and extending the theoretical, practical, and/or useful application of an idea, concept, or preliminary design. This also involves a plan for moving a project concept to a viable project.
Execute	The period within the project lifecycle during which the actual work of creating the	Involves directing, accomplishing, managing, and completing all phases and

Steps	Description	Process
	project's deliverables is carried out.	aspects of work for a given project.
Control	A mechanism which reacts to the current project status in order to ensure accomplishment of project objectives. This involves planning, measuring, monitoring, and taking corrective action based on the results of the monitoring.	Involves exercising corrective action as necessary to yield a required outcome consequent upon monitoring performance. Or, the process of comparing actual performance with planned performance, analyzing variances, evaluating possible alternatives, and taking appropriate correct action as needed.
Close Out	The completion of all work on a project. Can also refer to completion of a phase of the project.	Involves formally terminating and concluding all tasks, activities, and component parts of a particular project, or phase of a project.