

# FY 2020 HOMELAND SECURITY GRANT



## CITY OF VISALIA FIRE DEPARTMENT





# Office of Emergency Services

5957 South Mooney Boulevard, Visalia, California 93277  
(559) 624-8000 Telephone      (559) 624-7499 Facsimile

December 6, 2021

Dan Griswold  
Fire Chief  
City of Visalia, Fire Department  
420 N. Burke St  
Visalia CA 93292  
Dan.Griswold@visalia.city

**Subject: NOTIFICATION OF SUBRECIPIENT AWARD**

FY 2020 State Homeland Security Grant Program (SHSGP)  
Subaward #: 2020-0095, Cal OES ID: 107-00000, CFDA #: 97-067  
Subaward Period of Performance: 09/01/2020 to 05/31/2023

Dear Chief Griswold,

Please accept this letter as the official subaward notification for the Visalia Fire Department, DUNS #: 047898700, from the FY 2020 State Homeland Security Grant Program.

A summary of your subaward follows:

- **Project 010** – Hazmat Technician /Specialist Class Series (Training Consultant): \$34,000.
- **Project 011** – Hazmat Technician /Specialist Class Series (Travel): \$22,907.
- **Project 012** – Hazmat Technician /Specialist Class Series (Training Consultant): \$19,500.
- **Project 013** – Hazmat Technician /Specialist Class Series (Travel): \$11,453.

Please see the attached Grant Award Workbook page for the approved equipment and corresponding AEL number(s). Your agency has only been approved to purchase the equipment listed on the Grant Award Workbook page.

As a condition of funding, your agency must accept the Subaward Agreement Regarding FY 2020 State Homeland Security Grant Program Funding for Equipment, Planning, Administration, Training and Exercises. This agreement must be signed by your governing body and accompanied by a copy of the governing body's resolution accepting the agreement.

For all grant-funded procurement, your agency must adhere to the terms contained within the above-referenced agreement, all relevant State and Federal laws and regulations. In particular, you must adhere to the most restrictive procurement standard on each topic, for each procurement, between the following:

- a. Your jurisdiction's ordinances and formally adopted procurement policies.
- b. State law; and
- c. The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Title 2, Code of Federal Regulations [CFR] Part 200, including but not limited to such sections as 2 CFR §200.320 "Methods of procurement to be followed")

For activities flagged for additional review on the Grant Award Workbook page (e.g., Environmental Planning and Historic Preservation, Allowability Requests, Aviation, Performance Bond, etc.), your agency shall not incur costs until you and Tulare County OES receive written approval from Cal OES removing the hold.

This subaward is subject to all provisions of 2 CFR Part 200, including Subpart F - Audit Requirements. Any funds received in excess of current needs, approved amounts, or those found owed as a result of a final review or audit, must be refunded to the State within 30 days upon receipt of an invoice.

All activities, invoices, and payments for the awarded activities must be dated within the performance period to be eligible for reimbursement. Reimbursement requested after April 30 of each year may be delayed until the following Fiscal Year; please plan accordingly and be prepared to accrue reimbursement if submitting during this time.

The final deadline for completed reimbursement requests to be submitted is February 28, 2023, to allow time for grant close-out activities.

Requests for reimbursement, questions, or information requests should be submitted to the OES Grant Administrator at [OESGrants@tularecounty.ca.gov](mailto:OESGrants@tularecounty.ca.gov) or at:

Office of Emergency Services  
Tulare County HHSA  
5957 South Mooney Boulevard  
Visalia, California 93277

Sincerely Yours,



Andrew Lockman  
Emergency Services Manager

# 2020 HOMELAND SECURITY GRANT AWARD

SUBAWARD #: 2020-0095, CAL OES ID: 107-00000, CFDA #: 97-067

## EQUIPMENT AWARD FOR THE CITY OF VISALIA, FIRE DEPARTMENT

Project	Description & Quantity	AEL# / Feedback Number	AEL Title / Activity	Discipline	Proposed Vendor	Total Cost	Hold Trigger
010	Hazmat Technician Training			FS	California Specialized Training Institute	\$ 34,000	No
011	Hazmat Technician Training			FS	California Specialized Training Institute	\$ 22,907	No
012	Hazmat Specialist Training			FS	California Specialized Training Institute	\$ 19,500	No

013	Hazmat Technician/Specialist Class Series	Field-Based Attendee	FS	California Specialized Training Institute	\$ 11,453	No
<b>TOTAL AWARD AMOUNT</b>						<b>\$ 87,860</b>

# QUICK TIPS FOR HOMELAND SECURITY GRANT RECIPIENTS

**Do NOT purchase anything until you have received an award letter from Tulare County OES**

- You must conduct a search on the [System for Award Management \(SAM\)](#) website prior to entering into an agreement with any vendor for HSGP-related expenses. Verification must be provided (i.e. printed search results) upon submission of a reimbursement request to show that the vendor was not debarred or suspended during the time of service for your awarded project(s). If it is discovered that the vendor was debarred or suspended during that time, your project will not be reimbursed.
- If your project involves/requires a contract, you must provide the contractor a copy of the Cal OES Standard Grant Assurances for that grant cycle, and stipulate that they must abide by the terms of those assurances.
- Your project may be placed on [conditional hold](#) by the State even though the grant was approved. DO NOT proceed with any part of your award purchase until you receive authorization from Tulare County OES that the conditional hold has been released. This can be due to Sole Source or EHP reviews.
- All [invoices](#) must be dated after the date printed on the Tulare County OES award letter or they will not be reimbursed.
- You may only purchase the [equipment](#) listed on the Equipment Workbook page provided with your award letter. Any deviation from the approved equipment and/or AEL number will not be reimbursed.
- A [performance period](#) is issued for each project. The ending date of the performance period is the ending date of your award. No purchases are allowed after this date.
- [Environmental and Historic Preservation \(EHP\) reviews](#) must be approved before you initiate the purchasing process. If documentation shows that purchases occurred prior to receiving EHP approval, those purchases will not be reimbursed.
- All public safety communications equipment must be [P25-compliant](#). NO EXCEPTIONS.

- You must obtain a **performance bond** for any equipment item over \$250,000 or any vehicle, aircraft or watercraft, funded with HSGP funds.
- **Sole source procurements** in excess of \$100,000 must receive prior written approval. Interagency agreements between units of government are excluded from this provision.
- **Maintenance contracts and warranties** for equipment are allowable costs. You may purchase a maintenance contract or warranty at the time of procurement or at a later time to extend the useful life of the equipment. For example, you may purchase a maintenance contract or warranty from one fiscal year to cover equipment purchased with funding from a different fiscal year. Maintenance contracts must be purchased using funds from FEMA's preparedness grant programs. The term of the maintenance contract or warranty can exceed the period of performance of the grant to which the contract is being charged.
- Most equipment (technology or equipment costing over \$5,000) must be tagged with an **HSGP Inventory sticker** issued by Tulare County OES before reimbursement. If applicable to your project(s), you will receive a letter, sticker(s), and an inventory form to complete and return to Tulare County OES.
- Sub-Recipients are responsible for replacing or repairing property and equipment which is willfully or negligently lost, stolen, damaged, or destroyed. Any loss, damage, or theft of the property must be investigated and fully documented and made part of the official project records.
- Your equipment will be **inventoried** by Tulare County OES every two years, and compliance is required. If anything is missing, lost or stolen, your department is responsible to replace it. This does not apply to expendable items, such as gloves, masks or other expendable personal protective equipment.
- **Tips** will not be reimbursed.
- **Meals** will not be reimbursed without prior Cal OES approval.
- **Lodging** will be reimbursed according to the Federal per diem rates set for the County and the season. Lodging will not be reimbursed at all if the rate exceeds the amount allowed by the United States General Services Administration, accessible at [www.gsa.gov/perdiem](http://www.gsa.gov/perdiem).
- All **training** must be pre-approved and issued a training tracking number before any costs associated with that training can be incurred.
- **Training Certificates** must accompany your reimbursement request.

**TULARE COUNTY OFFICE OF EMERGENCY SERVICES  
SUB-GRANTEE PASSTHROUGH TO LOCAL REIMBURSEMENT REQUEST  
FY 2020 Homeland Security Grant Program (HSGP)  
Award# 2020- 0095 OES ID # 107-00000**

\* Reimbursement Request Checklist must be completed and submitted with this form to be eligible for reimbursement

## **REIMBURSEMENT REQUEST**

<b>SUB-RECIPIENT</b> _____	
<b>PROJECT #</b> (one per form) _____	<b>MICRO PURCHASE THRESHOLD</b> _____ \$ <i>(\$10,000 if unknown)</i>
<b>CLAIM AMOUNT</b> _____	<b>BID THRESHOLD</b> _____ \$ _____
<b>PROCUREMENT TYPE</b> (refer to 2 CFR 200.320 for definitions)	
<input type="checkbox"/> <b>Micro</b> (under \$10,000 or your Micro Threshold, whichever is higher)	
<input type="checkbox"/> <b>Small</b> (between \$10,000/your Micro Threshold and \$250,000/your Bid Threshold)	
<input type="checkbox"/> <b>Competitive</b> (over \$250,000+ or your Bid Threshold, whichever is lower)	
<input type="checkbox"/> <b>Non-Competitive</b> (per 2 CFR 200.320(c))	

Under penalty of perjury, I certify that:

*I am duly authorized officer of the claimant herein, that this claim is in all respects true, correct, and in accordance with applicable laws, rules, and regulations, that the services mentioned herein were actually rendered, and that I have not violated any of the provision of government Code Section 1090 to 1096, inclusive.*

### **AUTHORIZED AGENT**

Name _____	E-Mail Address _____ (559) _____
Title _____	Telephone Number _____ (559) _____
Mailing Address _____	Fax Number _____
City, State, Zip Code _____	_____
Signature _____	Date _____

Submit Reimbursement Request to:  
**Tulare County Office of Emergency Services**  
5957 S Mooney Blvd  
Visalia CA 93277  
559-624-7495 office  
[\(OESGrants@tularecounty.ca.gov\)](mailto:(OESGrants@tularecounty.ca.gov))

Date Received \_\_\_\_\_

\*\*

**TULARE COUNTY OFFICE OF EMERGENCY SERVICES  
SUB-GRANTEE PASSTHROUGH TO LOCAL REIMBURSEMENT REQUEST  
FY 2020 Homeland Security Grant Program (HSGP)  
Award# 2020-0095 OES ID # 107-00000**

## **REIMBURSEMENT REQUEST CHECKLIST**

### **SYSTEM FOR AWARDS MANAGEMENT (SAM)**

For all reimbursements, you MUST have verified, and MUST re-verify, that each vendor to whom payment was made is NOT listed for exclusion or debarment on the U.S. Government's "[System for Awards Management](#)" database. Sub-Recipients can verify the party's eligibility by going to the website <http://www.sam.gov> and searching for the party's name. **Print the party's result prior to purchase and submit it with the reimbursement request along with the report generated at the time of the Project Proposal.** If the party is listed for exclusion or debarment on the website, you will NOT be eligible for reimbursement.

### **REIMBURSEMENT ITEMIZATION**

ITEM(S)	INVOICE#	CHECK#	AMOUNT
<b>TOTAL</b>			<b>\$ 0.00</b>

### **ALL REIMBURSEMENTS**

Remit to OES:

- Vendor Quote(s):
  - Micro Purchases: Selected Quote
  - Small Purchases: Selected Quote **and** "an adequate number of price or rate quotations" – minimum 2 non-selected quotes for the same item (see 2 CFR 200.320(b))
  - Competitive Bid & Non-Competitive Procurements: All Bid documents, including specifications, advertisements, list of recipients (including minority & women owned businesses), all received bids, required analyses such as cost/price analysis, profit negotiation as separate component of cost (see generally, grant assurances and 2 CFR 200; notably, but not limited to, sections 318, 319, 320, 321, 322, 324, 326, and 327)

- Procurement history documentation, to include rationale for method of procurement, selection of contract type, contractor selection or rejection, and basis for the contract price (see 2 CFR 200.318(i))
- Completed Reimbursement Request packet (including this Checklist)
- **Contracts: Vendor contract with Federally Required terms incorporated.**
- Copies of all Invoices and Packing Slip(s)
- Copy of the “[System for Awards Management](#)” search results
- Copy of the canceled check(s) issued to pay the vendor(s) (front and back, legible)

## PLANNING PROJECTS

- Copies of all reports and deliverables (i.e. final product)
- 

## TRAINING REIMBURSEMENTS

- Complete and detailed Time Studies for any claimed personnel expenses
- **Vendor contract with Federally Required terms incorporated**
- Timecards of all personnel who received overtime\*, including rate of pay
- Timecards of all personnel used to backfill\*, including rate of pay
  - \* Overtime and backfill cannot overlap. Overtime and/or backfill are subject to **PRIOR** approval by the Approval Authority and/or Tulare County OES; approved on a case-by-case basis.
- Copies of payroll reports for each claimed pay period
- Copy of training CERTIFICATE(S) issued Copy of agenda or syllabus
- All receipts for travel, meals, lodging\*
  - \* Lodging is allowable up to the Federal Per Diem rate per <http://www.gsa.gov>. Lodging will NOT be reimbursed at all if the cost per night exceeds the Federal Per Diem rate. Tips are NOT reimbursable. Alcohol is not allowable. Meals for hosted training must be preapproved by Cal OES.

## EQUIPMENT PROJECTS

Serial numbers of equipment items and deployed address(es) where each item will be used or stored.

**TULARE COUNTY OFFICE OF EMERGENCY SERVICES  
SUB-GRANTEE PASSTHROUGH TO LOCAL REIMBURSEMENT REQUEST  
FY 2020 Homeland Security Grant Program (HSGP)  
Award# 2020-0095 OES ID # 107-00000**

OES will use the information submitted to provide an Equipment Inventory Tracking Sheet and Homeland Security Asset Tag(s):

- ❑ Complete the Equipment Inventory Tracking Sheet
- ❑ Apply the Homeland Security Asset Tag(s), if applicable
- ❑ Initial, sign and date the Equipment Inventory Tracking Sheet
- ❑ Remit the completed Equipment Inventory Tracking Sheet to OES

**The Department of Homeland Security (DHS)  
Notice of Funding Opportunity (NOFO)  
Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP)**

**NOTE:** If you are going to apply for this funding opportunity and have not obtained a Data Universal Numbering System (DUNS) number and/or are not currently registered in the System for Award Management (SAM), please take immediate action to obtain a DUNS Number, if applicable, and then to register immediately in SAM. It may take four weeks or more after you submit your SAM registration before your registration is active in SAM, then an additional 24 hours for Grants.gov to recognize your information. Information on obtaining a DUNS number and registering in SAM is available from Grants.gov at: <http://www.grants.gov/web/grants/register.html>.

**A. Program Description**

**1. Issued By**

Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Grant Programs Directorate (GPD)

**2. Assistance Listings Number (formerly Catalog of Federal Domestic Assistance Number) 97.067**

**3. Assistance Listings Title (formerly CFDA Title)**  
Homeland Security Grant Program

**4. Funding Opportunity Title**

Homeland Security Grant Program

- State Homeland Security Program
- Urban Area Security Initiative
- Operation Stonegarden

**5. Funding Opportunity Number**  
DHS-20-GPD-067-00-01

**6. Authorizing Authority for Program**

Section 2002 of the *Homeland Security Act of 2002* (Pub. L. No. 107-296, as amended) (6 U.S.C. § 603)

**7. Appropriation Authority for Program**

*Department of Homeland Security Appropriations Act, 2020* (Pub. L. No. 116-93)

**8. Announcement Type**

New

## 9. Program Overview, Objectives, and Priorities

### Overview

The Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP) is one of three grant programs that constitute the Department of Homeland Security (DHS)/Federal Emergency Management Agency's (FEMA's) focus on enhancing the ability of state, local, tribal, and territorial governments, as well as nonprofits, to prevent, protect against, respond to, and recover from terrorist attacks. These grant programs are part of a comprehensive set of measures authorized by Congress and implemented by DHS to help strengthen the Nation's communities against potential terrorist attacks. Among the five basic homeland security missions noted in the DHS Quadrennial Homeland Security Review, HSGP supports the goal to Strengthen National Preparedness and Resilience. In FY 2020, there are three components of HSGP:

- 1) ***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.
- 2) ***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.
- 3) ***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 inherent law enforcement authorities to support the border security mission and do not receive any additional authority as a result of participation in OPSG.

The 2018-2022 FEMA Strategic Plan creates a shared vision for reducing the risks posed by terrorism and sets an ambitious, yet achievable, path forward to unify and further professionalize emergency management across the country. HSGP supports the goals of Building a Culture of Preparedness and Readyng the Nation for Catastrophic Disasters. We invite our stakeholders and partners to also adopt these priorities and join us in building a more prepared and resilient Nation, as preparedness is a shared responsibility and funding should support priorities that are most impactful and demonstrate the greatest return on investment.

Finally, for FY 2020, DHS is focused on the criticality of information sharing and collaboration to building a national culture of preparedness and protecting against terrorism and other emerging threats to our national security. DHS and its homeland security mission were born from the “failures among federal agencies and between the federal agencies and state and local authorities to share critical information related to the threat of terrorism” prior to the September 11, 2001, attacks.<sup>1</sup> The threat profile has changed in the last two decades – we now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, threats to our democratic election

---

<sup>1</sup> Homeland Security Act of 2002: Report Together with Minority and Dissenting Views 222, Select Committee on Homeland Security: 107th Congress, U.S. House of Representatives (2002) (H. Rpt. 107-609).

process and threats from new and emerging technologies. But information sharing and cooperation between state, local, and tribal authorities and federal agencies, including all DHS officials, is just as vital, and perhaps even more vital, today. Therefore, for FY 2020, we have identified four priority areas, tied to some of the most serious threats that DHS would like to see addressed by state and local governments, that recipients will need to address with their HSGP funds. Perhaps most importantly, we will be focused on forging partnerships to strengthen information sharing and collaboration in each of these priority areas and looking for recipients to remove barriers to communication and cooperation with DHS and other federal agencies.

## **Objectives**

The objective of the FY 2020 HSGP is to fund state, local, tribal, and territorial efforts to prevent terrorism and prepare the Nation for threats and hazards that pose the greatest risk to the security of the United States.

## **Priorities**

Given the evolving threat landscape, it is incumbent upon DHS/FEMA to continuously evaluate the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2020, four priority areas attract the most concern. And due to the unique threats that the nation faces in 2020, DHS/FEMA has determined that these four priorities should be addressed by allocating specific percentages of HSGP funds to each of these four areas, for a total of 20 percent. The following are the four priority areas for FY 2020, along with the corresponding amount of HSGP funds that each recipient will be required to propose for each priority area in order to obtain a full allocation of HSGP funds:

- 1) Enhancing cybersecurity (including election security) – 5 percent
- 2) Enhancing the protection of soft targets/crowded places (including election security) – 5 percent;
- 3) Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS – 5 percent;
- 4) Addressing emergent threats (e.g., unmanned aerial systems [UASs], etc.) – 5 percent.

Failure by a recipient to propose investments and projects that align with these four priority areas and spending requirements may result in a recipient receiving a reduced grant award. DHS/FEMA may not award funding in excess of a recipient's minimum allocation threshold<sup>2</sup> to the extent that investments and projects do not align with these four priority areas.

A State or high-risk urban area may allocate the remaining 80 percent to gaps identified through their Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Process.

Likewise, there are several enduring security needs that crosscut the homeland security enterprise, and to which that States should consider allocating funding across core capability gaps and national

---

<sup>2</sup> The *Homeland Security Act of 2002*, as amended, allocates for each of the 50 States, the District of Columbia, and Puerto Rico 0.35 percent of the total funds appropriated for grants under section 2003 and section 2004 of the *Act*, and 0.08 percent for each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands).

priorities. The following are enduring needs that help recipients implement a comprehensive approach to securing communities:

- 1) Effective planning;
- 2) Training and awareness campaigns;
- 3) Equipment and capital projects; and
- 4) Exercises.

The table below provides a breakdown of the FY 2020 SHSP and UASI priorities (the focus of OPSG remains unique to border security), showing the core capabilities enhanced and lifelines supported, as well as examples of eligible project types for each area. A detailed description of allowable investments for each project type is included in the [Preparedness Grants Manual](#). DHS/FEMA anticipate that in future years, national priorities will continue to be included and will be updated as the threats evolve and as capability gaps are closed. Applicants are strongly encouraged to begin planning to sustain existing capabilities through other funding mechanisms.

#### **FY 2020 SHSP & UASI Funding Priorities**

Priority Areas	Core Capabilities	Lifelines	Example Project Types
<b>National Priorities</b>			
Enhancing Cybersecurity (including election security)	<ul style="list-style-type: none"> <li>• Cybersecurity</li> <li>• Intelligence and information sharing</li> </ul>	<ul style="list-style-type: none"> <li>• Safety and security</li> </ul>	<ul style="list-style-type: none"> <li>• Cybersecurity risk assessments</li> <li>• Projects that address vulnerabilities identified in cybersecurity risk assessments <ul style="list-style-type: none"> <li>◦ Improving cybersecurity of critical infrastructure to meet minimum levels identified by CISA</li> <li>◦ Cybersecurity training and planning</li> </ul> </li> </ul>
Enhancing the Protection of Soft Targets/ Crowded Places (including election security)	<ul style="list-style-type: none"> <li>• Operational coordination</li> <li>• Public information and warning</li> <li>• Intelligence and information sharing</li> <li>• Interdiction and disruption</li> <li>• Screening, search, and detection</li> <li>• Access control and identity verification</li> <li>• Physical protective measures</li> <li>• Risk management for protection programs and activities</li> </ul>	<ul style="list-style-type: none"> <li>• Safety and security</li> </ul>	<ul style="list-style-type: none"> <li>• Operational overtime</li> <li>• Physical security enhancements <ul style="list-style-type: none"> <li>◦ Security cameras (CCTV)</li> <li>◦ Security screening equipment for people and baggage</li> <li>◦ Lighting</li> <li>◦ Access controls</li> <li>◦ Fencing, gates, barriers, etc.</li> </ul> </li> </ul>
Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS	<ul style="list-style-type: none"> <li>• Intelligence and information sharing</li> </ul>	<ul style="list-style-type: none"> <li>• Safety and security</li> </ul>	<ul style="list-style-type: none"> <li>• Fusion center operations (Fusion Center project will be required under this investment, no longer as a stand-alone investment)</li> <li>• Information sharing with all DHS components, fusion centers, and other entities designated by DHS</li> </ul>

			<ul style="list-style-type: none"> <li>• Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis</li> <li>• Joint training and planning with DHS officials and other entities designated by DHS</li> </ul>
Addressing Emergent Threats, such as Transnational Criminal Organizations and UAS	<ul style="list-style-type: none"> <li>• Interdiction &amp; disruption</li> <li>• Screening, search and detection</li> <li>• Physical protective measures</li> <li>• Intelligence and information sharing</li> <li>• Planning</li> <li>• Public Information and Warning</li> <li>• Operational Coordination</li> </ul>	• Safety and security	<ul style="list-style-type: none"> <li>• Sharing and leveraging intelligence and information</li> <li>• UAS detection technologies</li> <li>• Enhancing weapons of mass destruction (WMD) and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities <ul style="list-style-type: none"> <li>◦ Chemical Biological Radiological Nuclear and Explosive (CBRNE) detection, prevention, response, and recovery equipment</li> </ul> </li> </ul>
<b>Enduring Needs</b>			
Planning	<ul style="list-style-type: none"> <li>• Planning</li> <li>• Risk management for protection programs and activities</li> <li>• Risk and disaster resilience assessment</li> <li>• Threats and hazards identification</li> <li>• Operational coordination</li> <li>• Community resilience</li> </ul>	• Safety and security	<ul style="list-style-type: none"> <li>• Development of: <ul style="list-style-type: none"> <li>◦ Security Risk Management Plans</li> <li>◦ Continuity of Operations Plans</li> <li>◦ Response Plans</li> </ul> </li> <li>• Efforts to strengthen governance integration between/among regional partners</li> <li>• Joint training and planning with DHS officials and other entities designated by DHS</li> <li>• Cybersecurity training and planning</li> </ul>
Training & Awareness	<ul style="list-style-type: none"> <li>• Long-term vulnerability reduction</li> <li>• Public information and warning</li> <li>• Operational coordination</li> <li>• Situational assessment</li> <li>• Community resilience</li> </ul>	• Safety and security	<ul style="list-style-type: none"> <li>• Active shooter training</li> <li>• Security training for employees</li> <li>• Public awareness/preparedness campaigns</li> <li>• Joint training and planning with DHS officials and other entities designated by DHS</li> <li>• Cybersecurity training and planning</li> </ul>
Equipment & Capital Projects	<ul style="list-style-type: none"> <li>• Long-term vulnerability reduction</li> <li>• Infrastructure systems</li> <li>• Operational communications</li> <li>• Interdiction and disruption</li> <li>• Screening, search and detection</li> <li>• Access control and identity verification</li> <li>• Physical protective measures</li> </ul>	• Safety and security	<ul style="list-style-type: none"> <li>• Protection of high-risk, high-consequence areas or systems that have been identified through risk assessments</li> <li>• Physical security enhancements <ul style="list-style-type: none"> <li>◦ Security cameras (CCTV)</li> <li>◦ Security screening equipment for people and baggage</li> <li>◦ Lighting</li> <li>◦ Access Controls <ul style="list-style-type: none"> <li>▪ Fencing, gates, barriers, etc.</li> </ul> </li> </ul> </li> </ul>

Exercises	<ul style="list-style-type: none"> <li>• Long-term vulnerability reduction</li> <li>• Operational coordination</li> <li>• Operational communications</li> <li>• Community resilience</li> </ul>	<ul style="list-style-type: none"> <li>• Safety and security</li> </ul>	<ul style="list-style-type: none"> <li>• Response exercises</li> </ul>
-----------	---	---	--

Starting in FY 2020, each SHSP and UASI recipient is required to submit an Investment Justification (IJ) for *each* of the four national priorities identified above. Under the Cybersecurity investment and the Soft Target/Crowded Places investments one project for each of those two investments must be to support enhancing election security. As a reminder, all SHSP- and UASI-funded projects must have a demonstrated nexus to preventing, preparing for, protecting against, and responding to acts of terrorism. However, such projects may simultaneously support enhanced preparedness for disasters unrelated to acts of terrorism.

DHS/FEMA also requires SHSP and UASI recipients (e.g., states, territories, and high-risk urban areas) to complete a THIRA/SPR and prioritize grant funding to support closing capability gaps or sustaining capabilities that address national priorities and/or support enduring needs. Additional information on the THIRA/SPR process, including other National Preparedness System (NPS) tools and resources, can be found at <https://www.fema.gov/national-preparedness-system>. Detailed information on THIRA/SPR timelines and deadlines can be found in the Preparedness Grants Manual.

### FY 2020 OPSG Funding Priorities

Priority Areas	Core Capabilities	Lifelines	Example Project Types
<b>National Priorities</b>			
Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS	<ul style="list-style-type: none"> <li>• Intelligence and information sharing</li> </ul>	<ul style="list-style-type: none"> <li>• Safety and security</li> </ul>	<ul style="list-style-type: none"> <li>• Participation in the DHS/ICE 287(g) training program</li> <li>• Information sharing with all DHS components, fusion centers, and other entities designated by DHS</li> <li>• Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis</li> <li>• Joint training and planning with DHS officials and other entities designated by DHS</li> </ul>
Addressing Emergent Threats, such as Transnational Criminal Organizations	<ul style="list-style-type: none"> <li>• Interdiction &amp; disruption</li> <li>• Screening, search and detection</li> <li>• Physical protective measures</li> <li>• Intelligence and information sharing</li> </ul>	<ul style="list-style-type: none"> <li>• Safety and security</li> </ul>	<ul style="list-style-type: none"> <li>• Operational overtime for border security operations as directed by the applicable, USBP-approved operations order</li> <li>• Sharing and leveraging intelligence and information</li> </ul>

Starting in FY 2020, each OPSG applicant is required to clearly articulate and identify how the Concept of Operations addresses *each* of the two national priorities identified above.

## 10. Performance Metrics

Performance metrics for this program are as follows:

SHSP and UASI:

- Percentage of funding allocated by the recipient to core capabilities to build or sustain national priorities identified in the section above; and

OPSG:

- Number of contacts that occurred as a result of OPSG deployments
  - Number of arrests that resulted from OPSG contacts
  - Value of drug seizures that resulted from OPSG contacts

## **B. Federal Award Information**

### **Award Amounts, Important Dates, and Extensions**

**Available Funding for the HSGP NOFO: \$1,120,000,000**

HSGP Programs	FY 2020 Allocation
State Homeland Security Program	\$415,000,000
Urban Area Security Initiative	\$615,000,000
Operation Stonegarden	\$90,000,000
<b>Total</b>	<b>\$1,120,000,000</b>

### **SHSP Allocations**

For FY 2020, DHS/FEMA will award SHSP funds based on risk and the anticipated effectiveness of the proposed use of grant funds upon completion of the application review process. The following table identifies the *targeted* SHSP allocation ranges for each State based on DHS/FEMA's relative risk methodology pursuant to the *Homeland Security Act of 2002*, as amended. States are strongly encouraged to apply for funding at least 15% over the high end of their target allocation range as ineffective applications will not be funded. Final award amounts will be based on DHS/FEMA's evaluation of the effectiveness of proposed investments and projects.

Regardless of the amount of a State's targeted SHSP allocation range, each State must include a separate investment for each of the four national priority areas identified in the Priorities section, above. The funding level in each national priority area investment must equal or exceed the percentage for that respective national priority area, calculated as a percentage of the State's *targeted* SHSP allocation in the table below. For the states that receive a target allocation in excess of the minimum, the percentage is calculated against the high end of the range, as displayed in the table below. DHS/FEMA will make final award determinations based upon a review of the anticipated effectiveness of the State's application as described in Section D, below. Final awards are based on whether the State has proposed investments in each of the four national priority areas in an amount equal to or greater than the percentage for that priority area and based on the effectiveness review.

DHS/FEMA will allocate to each state and territory a minimum allocation under the SHSP using thresholds established in the *Homeland Security Act of 2002*, as amended. The minimum allocation for all 50 States, the District of Columbia, and the Commonwealth of Puerto Rico is 0.35 percent of the total funds appropriated for grants under Section 2003 and Section 2004 of the *Homeland Security Act of 2002*, as amended. The minimum allocation for the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) is 0.08 percent of the total funds appropriated for grants under Section 2003 and 2004 of the *Homeland Security Act of 2002*, as amended. THIRA/SPR results do not impact grant allocation or award.

Regardless of the final award amount, a state must invest SHSP funding in each of the four national priority areas in an amount equal to or greater than percentage identified above for each national priority area, as approved by DHS/FEMA.

### **FY 2020 TARGET SHSP ALLOCATIONS**

<b>State/Territory</b>	<b>FY 2020 Allocation</b>	<b>State/Territory</b>	<b>FY 2020 Allocation</b>
New York	\$59,174,400 - \$73,968,000	Kentucky	\$4,287,500
California	\$49,608,800 - \$62,011,000	Louisiana	\$4,287,500
Texas	\$15,839,200 - \$19,799,000	Maine	\$4,287,500
Illinois	\$12,085,600 - \$15,107,000	Minnesota	\$4,287,500
Florida	\$8,127,200 - \$10,159,000	Mississippi	\$4,287,500
Virginia	\$7,076,800 - \$8,846,000	Missouri	\$4,287,500
Georgia	\$4,600,000 - \$5,750,000	Montana	\$4,287,500
Pennsylvania	\$7,076,800 - \$8,846,000	Nebraska	\$4,287,500
Maryland	\$6,153,600 - \$7,692,000	Nevada	\$4,287,500
New Jersey	\$6,153,600 - \$7,692,000	New Hampshire	\$4,287,500
Washington	\$5,384,800 - \$6,731,000	New Mexico	\$4,287,500
Massachusetts	\$5,384,800 - \$6,731,000	North Dakota	\$4,287,500
Ohio	\$5,384,800 - \$6,731,000	Oklahoma	\$4,287,500
North Carolina	\$4,423,200 - \$5,529,000	Oregon	\$4,287,500
District of Columbia	\$4,423,200 - \$5,529,000	Puerto Rico	\$4,287,500
Michigan	\$4,423,200 - \$5,529,000	Rhode Island	\$4,287,500
Alabama	\$4,287,500	South Carolina	\$4,287,500
Alaska	\$4,287,500	South Dakota	\$4,287,500
Arizona	\$4,287,500	Tennessee	\$4,287,500
Arkansas	\$4,287,500	Utah	\$4,287,500
Colorado	\$4,287,500	Vermont	\$4,287,500
Connecticut	\$4,287,500	West Virginia	\$4,287,500
Delaware	\$4,287,500	Wisconsin	\$4,287,500
Hawaii	\$4,287,500	Wyoming	\$4,287,500
Idaho	\$4,287,500	American Samoa	\$1,000,000
Indiana	\$4,287,500	Guam	\$1,000,000
Iowa	\$4,287,500	Northern Mariana	\$1,000,000
Kansas	\$4,287,500	U.S. Virgin Islands	\$1,000,000
			<b>\$415,000,000</b>

## **UASI Allocations**

Eligible candidates for the FY 2020 UASI program are identified in the table below. Eligibility has been determined through an analysis of relative risk of terrorism faced by the 100 most populous Metropolitan Statistical Areas (MSAs) in the United States, in accordance with the *Homeland Security Act of 2002*, as amended. Detailed information on MSAs is publicly available from the United States Census Bureau at <https://www.census.gov/programs-surveys/metro-micro.html>. THIRA/SPR results do not impact grant allocation or award.

For FY 2020, DHS/FEMA will award UASI funds based on risk and the anticipated effectiveness of the proposed use of grant funds upon completion of the application review process. The following table identifies the *targeted* UASI allocations for each high-risk urban area based on DHS/FEMA's relative risk methodology pursuant to the *Homeland Security Act of 2002*, as amended. Applicants are strongly encouraged to apply for funding at least 15% over the high end of their target allocation range as ineffective applications will not be funded. Final award amounts will be based on DHS/FEMA's evaluation of the effectiveness of proposed investments and projects.

In its application, each high-risk urban area, through the State, must include a separate investment for each of the four national priority areas identified in the Priorities section, above. The funding level in each national priority area investment must equal or exceed the percentage for that respective national priority area, calculated as a percentage of the high-risk urban area's *targeted* UASI allocation in the table below. The percentage is calculated against the high end of the range, as displayed in the table below. DHS/FEMA will make final award determinations based upon a review of the anticipated effectiveness of the high-risk urban area's application as described in Section D, below. Final awards are based on whether the State has proposed investments in each of the four national priority areas in an amount equal to or greater than the percentage for that priority area and based on the effectiveness review. Regardless of the final award amount, a high-risk urban area must invest UASI funding in each of the four national priority areas in an amount equal to or greater than percentage identified above for each national priority area, as approved by DHS/FEMA.

## FY 2020 TARGET UASI ALLOCATIONS

State/Territory	Funded Urban Area	FY 2020 UASI Allocation
Arizona	Phoenix Area	\$4,200,000 - \$5,250,000
California	Anaheim/Santa Ana Area	\$4,200,000 - \$5,250,000
	Bay Area	\$30,000,000 - \$37,500,000
	Los Angeles/Long Beach Area	\$54,400,000 - \$68,000,000
	Riverside Area	\$2,800,000 - \$3,500,000
	Sacramento Area	\$2,800,000 - \$3,500,000
	San Diego Area	\$13,520,000 - \$16,900,000
Colorado	Denver Area	\$2,800,000 - \$3,500,000
District of Columbia	National Capital Region	\$41,400,000 - \$51,750,000
Florida	Miami/Fort Lauderdale Area	\$11,800,000 - \$14,750,000
	Orlando Area	\$2,800,000 - \$3,500,000
	Tampa Area	\$2,800,000 - \$3,500,000
Georgia	Atlanta Area	\$5,000,000 - \$6,250,000
Hawaii	Honolulu Area	\$2,800,000 - \$3,500,000
Illinois	Chicago Area	\$54,400,000 - \$68,000,000
Louisiana	New Orleans Area	\$2,800,000 - \$3,500,000
Maryland	Baltimore Area	\$3,400,000 - \$4,250,000
Massachusetts	Boston Area	\$13,520,000 - \$16,900,000
Michigan	Detroit Area	\$4,200,000 - \$5,250,000
Minnesota	Twin Cities Area	\$4,200,000 - \$5,250,000
Missouri	St. Louis Area	\$2,800,000 - \$3,500,000
Nevada	Las Vegas Area	\$4,200,000 - \$5,250,000
New Jersey	Jersey City/Newark Area	\$15,240,000 - \$19,050,000
New York	New York City Area	\$143,000,000 - \$178,750,000
Oregon	Portland Area	\$2,800,000 - \$3,500,000
Pennsylvania	Philadelphia Area	\$13,520,000 - \$16,900,000
	Pittsburgh Area	\$2,800,000 - \$3,500,000
Texas	Dallas/Fort Worth/Arlington Area	\$13,520,000 - \$16,900,000
	Houston Area	\$19,680,000 - \$24,600,000
	San Antonio Area	\$2,800,000 - \$3,500,000
Virginia	Hampton Roads Area	\$2,800,000 - \$3,500,000
Washington	Seattle Area	\$5,000,000 - \$6,250,000
<b>Total</b>		<b>\$615,000,000</b>

### OPSG Allocations

For FY 2020, DHS/FEMA will award OPSG funds based on risk and the anticipated effectiveness of the proposed use of grant funds upon completion of the application review process. The FY 2020 OPSG risk assessment is designed to identify the risk to border security and to assist with the distribution of funds for the grant program. Funding under OPSG is distributed based on the risk to the security of the border and the effectiveness of the proposed projects. Entities eligible for funding are the state, local, and tribal law enforcement agencies

that are located along the border of the United States. DHS/FEMA will make final award determinations based upon a review of the anticipated effectiveness of the State's application as described in Section D, below. The THIRA/SPR process is not required for OPSG.

For the purposes of OPSG, the risk is defined as the potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.

Based upon ongoing intelligence analysis and extensive security reviews, DHS/CBP continues to focus the bulk of OPSG funds based upon risk analyses. The risk model used to allocate OPSG funds considers the potential risk that certain threats pose to border security and estimates the relative risk faced by a given area. In evaluating risk, DHS/CBP considers intelligence, situational awareness, criminal trends, and statistical data specific to each of the border sectors, and the potential impacts that these threats pose to the security of the border area. For vulnerability and consequence, DHS/CBP considers the expected impact and consequences of successful border events occurring in specific areas.

Threat and vulnerability are evaluated based on specific operational data from DHS/CBP. Threat components present in each of the sectors are used to determine the overall threat score. These components are terrorism, criminal aliens, drug trafficking organizations, and alien smuggling organizations.

Effectiveness of the proposed investments will be evaluated based on the recipient's investment strategy, budget, collaboration, and past performance.

**Period of Performance:** 36 months

Extensions to the Period of Performance (PoP) are allowed. For additional information on PoP extensions, refer to the [Preparedness Grants Manual](#).

**Projected Period of Performance Start Date:** September 1, 2020

**Projected Period of Performance End Date:** August 31, 2023

**Funding Instrument:** Grant

## **C. Eligibility Information**

### **1. Eligible Applicants**

The State Administrative Agency (SAA) is the only entity eligible to submit HSGP applications to DHS/FEMA, including those applications submitted on behalf of UASI and OPSG applicants. All 56 states and territories, including any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, are eligible to apply for SHSP funds. Tribal governments may not apply directly for HSGP funding; however, funding may be available to tribes under the SHSP and OPSG through the SAA.

### **2. Eligibility Criteria**

Eligible high-risk urban areas for the FY 2020 UASI program have been determined through

an analysis of relative risk of terrorism faced by the 100 most populous Metropolitan Statistical Areas (MSAs) in the United States. Subawards will be made by the SAAs to the designated high-risk urban areas.

In FY 2020, OPSG eligible subrecipients are local units of government at the county level or equivalent level of government and Federally recognized tribal governments in states bordering Canada or Mexico and states and territories with international water borders. All applicants must have active ongoing USBP operations coordinated through a CBP sector office to be eligible for OPSG funding.

In FY 2020, OPSG subrecipients eligible to apply for and receive a subaward directly from the SAAs are divided into three Tiers. Tier 1 entities are local units of government at the county level or equivalent and Federally recognized tribal governments that are on a physical border in states bordering Canada, states bordering Mexico, and states and territories with international water borders. Tier 2 eligible subrecipients are those not located on the physical border or international water but are contiguous to a Tier 1 county. Tier 3 eligible subrecipients are those not located on the physical border or international water but are contiguous to a Tier 2 eligible subrecipient. The tier structure is only applicable with regard to eligibility. OPSG funding allocations are based on the assessed border security risks as determined by the USBP.

### **3. Other Eligibility Criteria**

#### **National Incident Management System (NIMS) Implementation**

Prior to allocation of any Federal preparedness awards in FY 2020, recipients must ensure and maintain adoption and implementation of NIMS. Detailed information on NIMS requirements are in the [Preparedness Grants Manual](#).

#### **Emergency Management Assistance Compact (EMAC) Membership**

In support of the Goal, SHSP recipients must belong to, be in, or act as a temporary member of EMAC, except for American Samoa and the Commonwealth of the Northern Mariana Islands, which are not required to belong to EMAC at this time. All assets supported in part or entirely with FY 2020 HSGP funding must be readily deployable and NIMS-typed when possible to support emergency or disaster operations per existing EMAC agreements. In addition, funding may be used for the sustainment of core capabilities that, while they may not be physically deployable, support national response capabilities, such as Geographic/Geospatial Information Systems (GIS), interoperable communications systems, capabilities as defined under the Mitigation Mission Area of the Goal, and fusion centers.

#### **Law Enforcement Terrorism Prevention Activities (LETPA)**

Per section 2006 of the *Homeland Security Act of 2002*, as amended (6 U.S.C. § 607), DHS/FEMA is required to ensure that at least 25 percent of grant funding appropriated for grants awarded under HSGP's authorizing statute are used for law enforcement terrorism prevention activities. DHS/FEMA meets this requirement, in part, by requiring all recipients allocate at least 25 percent of the combined HSGP funds allocated under SHSP and UASI towards law enforcement terrorism prevention activities, as defined in 6 U.S.C. § 607. The LETPA allocation can be from SHSP, UASI, or both. The 25 percent LETPA allocation may be met by funding projects in any combination of the four national priority areas

identified above and any other investments. And the 25 percent LETPA allocation is in addition to the 80 percent pass-through requirement to local units of government and tribes, referenced below.

The National Prevention Framework describes those activities that should be executed upon the discovery of intelligence or information regarding an imminent threat to the homeland, to thwart an initial or follow-on terrorist attack and provides guidance to ensure the Nation is prepared to prevent, avoid, or stop a threatened or actual act of terrorism. Activities outlined in the National Prevention Framework are eligible for use as LETPA-focused funds. Also, where capabilities are shared with the protection mission area, the National Protection Framework activities are also eligible. All other terrorism prevention activities proposed for funding under LETPA must be approved by the FEMA Administrator.

#### **4. Cost Share or Match**

There is no cost share or match requirement for the FY 2020 HSGP.

### **D. Application and Submission Information**

#### **1. Key Dates and Times**

- a. Application Start Date:** **February 14, 2020**
- b. Application Submission Deadline:** **April 30 15, 2020 at 5:00 p.m. ET**

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 the full application. **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, or other exigent or emergency circumstances.

**Applicants experiencing technical issues must notify the FEMA Headquarters (HQ) Program Analyst prior to the application deadline.** If applicants do not know their FEMA HQ 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](mailto:askcsid@fema.dhs.gov), Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

- c. Anticipated Funding Selection Date:** *No later than 7/1/2020*
- d. Anticipated Award Date:** *No later than 9/30/2020*
- e. Other Key Dates:**

Event	Suggested Deadline for Completion
Obtain DUNS Number	3/16/2020 3/1/2020
Obtain a valid Employer Identification Number (EIN)	3/16/2020 3/1/2020
Update SAM registration	3/16/2020 3/1/2020
Submit the initial application in Grants.gov	4/23/2020 4/8/2020
Submit the final application in ND Grants	4/30/2020 4/15/2020, 5:00 p.m. ET

## 2. Agreeing to Terms and Conditions of the Award

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

## 3. Address to Request Application Package

See the [Preparedness Grants Manual](#) for information on requesting and submitting an application.

## 4. Steps Required to Submit an Application, Unique Entity Identifier, and System for Award Management (SAM)

To apply for an award under this program, all applicants must:

- a. Apply for, update, or verify their Data Universal Numbering System (DUNS) Number from Dun & Bradstreet (D&B) and Employer ID Number (EIN)
- b. In the application, provide a valid Data Universal Numbering System DUNS number, which is currently the unique entity identifier;
- c. Have an account with [login.gov](#);
- d. Register for, update, or verify their SAM account and ensure the account is active before submitting the application;
- e. Create a Grants.gov account;
- f. Add a profile to a Grants.gov account;
- a. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
- b. Submit an initial application in Grants.gov;
- g. Submit the final application in the Non-Disaster Grants (ND Grants) system and
- h. 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.

Applicants are advised that DHS 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 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 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. See the [Preparedness Grants Manual](#) for additional information on the steps required to submit an application.

**5. 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 final applications through [ND Grants](#).

**6. How to Register to Apply through [Grants.gov](#)**

See the [Preparedness Grants Manual](#) for information on requesting and submitting an application.

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

See the [Preparedness Grants Manual](#) for information on requesting and submitting an application.

**8. Timely Receipt Requirements and Proof of Timely Submission**

As application submission is a two-step process, the applicant with the Authorized Organizational Representative (AOR) role who submitted the application will also receive an acknowledgement of receipt, a tracking number (in this format: GRANTXXXXXXXXXX) from Grants.gov, and an Agency Tracking Number (in this format: EMX-2020-XX-XXXX) with the successful transmission of the 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 p.m. ET on April 30 ~~15~~, 2020. 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.

**9. 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 but no later than **seven days before the application deadline**. Early registration will allow applicants to have adequate time to start and complete their application.

In [ND Grants](#) applicants will be prompted to submit all of the information contained in the following forms. Applicants should review these forms before applying to ensure they have all the information required:

- Standard Form 424A, Budget Information (Non-construction);
- Standard Form 424B, Standard Assurances (Non-construction); and
- Standard Form LLL, Disclosure of Lobbying Activities.

In addition, applicants must submit copies of the following in [ND Grants](#):

- Investment Justification (the Investment Justification Template may be found in the Related Documents Tab of the [Grants.gov](#) posting and used as a preparation tool; responses to questions in the Template are entered into the GRT);

- List of Urban Area Working Group (UAWG) and Senior Advisory Committee (SAC) members;
- SAC charter;
- UAWG charter; and
- Indirect Cost Agreement, 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.

Applicants must submit copies of the following in ND Grants if applying for construction projects. The forms may be accessed in the Forms tab under SF-424 Family on [Grants.gov](https://www.grants.gov):

- Standard Form 424C, Budget Information (Construction); and
- Standard Form 424D, Standard Assurances (Construction).

Applicants needing assistance registering for the ND Grants system should contact [ndgrants@fema.gov](mailto:ndgrants@fema.gov) or (800) 865-4076, Monday through Friday, 9 a.m. – 5 p.m. ET.

## 10. Content and Form of Application Submission

See the [Preparedness Grants Manual](#) for information on requesting and submitting an application.

### HSGP Specific Application Instructions

#### Development of the Investment Justification (SHSP and UASI)

As part of the FY 2020 HSGP application process for SHSP and UASI funds, applicants must develop formal investment justifications (IJs) that address the proposed investments. Failure to fulfill of all of the terms contained in this section will be considered by DHS/FEMA in its evaluation of the effectiveness of the IJs in accordance with the Risk Methodology and Effectiveness Review described in the Application Review Information and may result in rejection of proposed investments or reduced funding allocations.

Each IJ must *demonstrate* how proposed investments:

- Support terrorism preparedness;
- Support closing capability gaps or sustaining capabilities identified in the community's THIRA/SPR process; and
- Support the overcoming of existing logistical, technological, legal, policy, and other impediments to collaborating, networking, sharing information, cooperating, and fostering a culture of national preparedness with federal, state, tribal, and local governments, as well as other regional, and nonprofit partners in efforts to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, support the national security mission of DHS and other federal agencies, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.

Each IJ must *explain* how the proposed investments will support the applicant's efforts to:

- Prevent a threatened or an actual act of terrorism;
- Prepare for all hazards and threats, while explaining the nexus to terrorism preparedness;
- Protect citizens, residents, visitors, and assets against the greatest threats and hazards, relating to acts of terrorism; and/or
- Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of an act of terrorism or other catastrophic incidents.

### **Development of Investments and Projects (SHSP)**

- Applicants must propose at least four and may include up to ten investments.
- Required national priority investment justifications must include the name of the priority in the investment name for easy identification.
- Within each investment in their IJ, applicants must propose at least one project to describe the activities they plan to implement with SHSP funds. There is no limit to the number of projects that may be submitted.
- Of the proposed SHSP-funded investments, one single project, within the required intelligence and information sharing investment, must be in support of a designated fusion center. Recipients must coordinate with the fusion center when developing a fusion center project prior to submission. See additional information on how to develop the fusion center projects below.
- Of the proposed SHSP-funded investments, one project in each of the required Cybersecurity and Soft Targets/Crowded Places investments must be in support of enhancing election security.
- All emergency communications investments must describe how such activities align with their Statewide Communication Interoperable Plan (SCIP). Recipients must coordinate with their Statewide Interoperability Coordinator (SWIC) and/or Statewide Interoperability Governance Body (SIGB) when developing an emergency communications investment prior to submission to ensure the project supports the statewide strategy to improve emergency communications and is compatible and interoperable with surrounding systems. The investment name must include the words “emergency communications” to easily identify any emergency communications investments.
- All requested funding must be associated with specific projects. For each project, several pieces of information must be provided to submit the project for consideration in the application, including the name of the project, the project description, the name of the subrecipient, if applicable, the recipient type (e.g., state or local), the project location (zip code of the primary location of the project), the primary core capability the project supports, whether the project activities are shareable and deployable, and which priority area (if any) the project is in support of. Projects should describe how the proposed investment supports closing capability gaps or sustaining capabilities identified in the THIRA/SPR process. Failure to fulfill of all of the terms contained in this section may be considered in the evaluation of the effectiveness of the IJs in accordance with the Risk Methodology and Effectiveness Review described in the Application Review Information and may result in rejection of proposed investments or reduced funding allocations.
- FEMA encourages states to use any DHS provided assessments, such as those performed

by DHS's Protective Security Advisors and Cybersecurity Advisors, when developing their investment justifications.

### **Priority Investments (SHSP)**

States are encouraged to review the [Strategic Framework for Countering Terrorism and Targeted Violence](#) when developing investments.

### **Cybersecurity Investment Justification (5 percent)**

At least one investment must be in support of the state's cybersecurity efforts. The investment must meet or exceed the FY 2020 national priority percentage for cybersecurity, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of SHSP funds. Cybersecurity investments must support the security and functioning of critical infrastructure and core capabilities as they relate to preventing, preparing for, protecting against, or responding to acts of terrorism. Recipients and subrecipients of FY 2020 HSGP grant awards will be required to complete the 2020 [Nationwide Cybersecurity Review](#) (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The CIO, CISO or equivalent for each recipient should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2-3 hours to complete. The 2020 NCSR will be open from October – December 2020.

- The NCSR is an annual requirement for recipients and subrecipients of HSGP funds. Additionally, FEMA recognizes that some subawards will not be issued until after the NCSR has closed. In such cases, such subrecipients will be required to complete the first available NCSR offered after the subaward has been issued by the pass-through entity.
- Although not required by SLTTs that did not receive HSGP funds, all SLTT agencies with preparedness responsibilities are highly encouraged to participate and complete the NCSR to evaluate their cybersecurity posture. For detailed information and background on the NCSR, please see Information Bulletin 439.

In January 2017, the Department of Homeland Security designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Securing election infrastructure and ensuring an election free from foreign interference are national security priorities. Threats to election systems are constantly evolving, so defending these systems requires constant vigilance, innovation, and adaptation.

Given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the [Cybersecurity and Infrastructure Security Agency](#).

### **Soft Target Investment Justification (5 percent)**

Soft targets and crowded places are increasingly appealing to terrorists and other extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities.

Given the increased risk to soft targets and crowded places, at least one investment must be in support of the state's efforts to protect soft targets/crowded places. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for soft targets/crowded places and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments in order to receive a full allocation of SHSP funds. Additional resources and information regarding securing soft targets and crowded places are available through the [Cybersecurity and Infrastructure Security Agency](#). States are encouraged to engage DHS' Protective Security Advisors' security assessments of soft targets to ensure that recommendations from those assessments are taken into consideration when allocating grant funding.

As noted above, given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the [Cybersecurity and Infrastructure Security Agency](#).

### **Information Sharing and Cooperation Investment Justification (5 percent)**

Effective homeland security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Given the importance of information sharing and collaboration to effective homeland security solutions, at least one investment must be in support of the state's efforts to enhance information sharing and cooperation with DHS and other federal agencies. As noted above, this requirement must include at least one dedicated fusion center project. Additional instructions on development of the fusion center project can be found below. Applicants must justify persuasively how they

will contribute to the information sharing and collaboration purposes of the investment and a culture of national preparedness, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for information sharing and cooperation with DHS, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of SHSP funds. Additional resources and information regarding collaboration and information sharing are available through the Department's [Office of Intelligence and Analysis](#).

### **Emerging Threats Investment Justification (5 percent)**

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and no-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

Given the increased risk of emerging threats, at least one investment must be in support of the state's efforts to address emerging threats. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for emerging threats, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of SHSP funds. Additional resources and information regarding emerging threats are available through the [Countering Weapons of Mass Destruction Office](#) and the [Cybersecurity and Infrastructure Security Agency](#).

### **Development of Investments and Projects (UASI)**

- Applicants must propose at least four and may include up to ten investments.
- Within each investment in their IJ, Urban Areas must propose at least one project to describe the activities they are planning to implement with UASI funds. There is no limit to the number of projects that may be submitted.
- Required national priority IJs must include the name of the priority in the investment name for easy identification.
- Of the proposed projects, Urban Areas are required to propose one single project, as part of the required intelligence and information sharing investment justification, in support of a designated fusion center within the Urban Area, if applicable. Recipients must coordinate with the fusion center when developing a fusion center project prior to submission. See additional information on how to develop fusion center investments below.
- Of the proposed UASI-funded investments, one project in each of the required Cybersecurity and Soft Targets/Crowded Places investments, must be in support of enhancing election security.

All emergency communications investments must describe how such activities align with their Statewide Communication Interoperable Plan (SCIP). Recipients must coordinate with their Statewide Interoperability Coordinator (SWIC) and/or Statewide Interoperability Governance Body (SIGB) when developing an emergency communications investment prior to submission to ensure the project supports the statewide strategy to improve emergency communications and is compatible and interoperable with surrounding systems. The investment name must include the words “emergency communications” to easily identify any emergency communications investments.

All requested funding must be associated with specific projects. For each project, several pieces of information must be provided to submit the project for consideration in the application, including the name of the project, the project description, the name of the subrecipient, if applicable, the recipient type (e.g., state or local), the project location (zip code of the primary location of the project), the primary core capability the project supports, whether the project activities are shareable and deployable, and which priority area (if any) the project is in support of. Projects should describe how the proposed investment supports closing capability gaps or sustaining capabilities identified in the THIRA/SPRprocess

### **Priority Investments - UASI**

High-risk urban areas are encouraged to review the [Strategic Framework for Countering Terrorism and Targeted Violence](#) when developing investments.

### **Cybersecurity Investment Justification (5 percent)**

At least one investment must be in support of the urban area’s cybersecurity efforts. The investment must meet or exceed the FY 2020 national priority percentage for cybersecurity, and will also be subject to DHS/FEMA’s evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI and SHSP funds. Cybersecurity investments must support the security and functioning of critical infrastructure and core capabilities as they relate to preventing, preparing for, protecting against, or responding to acts of terrorism. Recipients and subrecipients of FY 2020 HSGP awards will be required to complete the 2020 [Nationwide Cybersecurity Review](#) (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The CIO, CISO or equivalent for each recipient should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. The NCSR is available at no cost to the user and takes approximately 2- 3 hours to complete. The 2020 NCSR will be open from October – December 2020.

- The NCSR is an annual requirement for recipients and subrecipients of HSGP funds. Additionally, FEMA recognizes that some subawards will not be issued until after the NCSR has closed. In such cases, such subrecipients will be required to complete the first available NCSR offered after the subaward has been issued by the pass-through entity.
- Although not required by SLTTs that did not receive HSGP funds, all SLTT agencies with preparedness responsibilities are highly encouraged to participate and complete the NCSR to evaluate their cybersecurity posture. For detailed information and background on the NCSR, please see Information Bulletin 439.

In January 2017, the Department of Homeland Security designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. Securing election infrastructure and ensuring an election free from foreign interference are national security priorities. Threats to election systems are constantly evolving, so defending these systems requires constant vigilance, innovation, and adaptation.

Given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the [Cybersecurity and Infrastructure Security Agency](#).

### **Soft Target Investment Justification (5 percent)**

Soft targets and crowded places are increasingly appealing to terrorists and other extremist actors because of their relative accessibility and the large number of potential targets. This challenge is complicated by the prevalent use of simple tactics and less sophisticated attacks. Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities.

Given the increased risk to soft targets and crowded places, at least one investment must be in support of the urban area's efforts to protect soft targets/crowded places. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for soft targets/crowded places and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI funds. Additional resources and information regarding securing soft targets and crowded places are available through the [Cybersecurity and Infrastructure Security Agency](#).

As noted above, given the importance of the Nation's election infrastructure, and the multiple and evolving threats to that infrastructure, at least one project within this investment must be in support of the state's efforts to enhance election security. Additional resources and information regarding election security are available through the [Cybersecurity and Infrastructure Security Agency](#).

### **Information Sharing and Cooperation Investment Justification (5 percent)**

Effective homeland security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is

critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Given the importance of information sharing and collaboration to effective homeland security solutions, at least one investment must be in support of the urban area's efforts to enhance information sharing and cooperation with DHS and other federal agencies. As noted above, this requirement must include at least one dedicated fusion center project. Additional instructions on development of the fusion center project can be found below. Applicants must justify persuasively how they will contribute to the information sharing and collaboration purposes of the investment and a culture of national preparedness, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for information sharing and cooperation with DHS, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI funds. Additional resources and information regarding collaboration and information sharing are available through the Department's [Office of Intelligence and Analysis](#).

### **Emerging Threats Investment Justification (5 percent)**

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

Given the increased risk of emerging threats, at least one investment must be in support of the urban area's efforts to address emerging threats. Additionally, the proposed investment must meet or exceed the FY 2020 national priority percentage for emerging threats, and will also be subject to DHS/FEMA's evaluation of the effectiveness of the proposed investments, in order to receive a full allocation of UASI funds. Additional resources and information regarding emerging threats are available through the [Countering Weapons of Mass Destruction Office](#) and the [Cybersecurity and Infrastructure Security Agency](#).

### **Development of Fusion Center Projects (SHSP and UASI)**

If applicable, each applicant must identify a fusion center project that will:

- Indicate alignment to a designated Fusion Center.
- Provide both a brief narrative description and funding itemization for the proposed project activities that directly support the designated fusion center.
- The descriptive narrative and the financial itemization should align improvement or sustainment requests with fusion center activities as they relate to the Fusion Center Performance Measures found in the Preparedness Grants Manual.

- If the project description and funding itemization do not directly support the fusion center or clearly align to the Fusion Center Performance Measures, then the project may be conditionally approved until a Fusion Center Addendum is submitted.

### ***Sample Fusion Center Funding Itemization***

A sample project description and funding itemization are below. For the itemized projects, clearly identify the anticipated fusion center performance improvement or sustainment as a result of the proposed funding.

*The X Fusion enhancement project will fund:*

- *Salaries, benefits, and training for X number of Fusion Center intelligence analysts*
- *Travel costs associated with fusion center analyst training.*
- *This project will directly sustain the Center's current capabilities and performance and directly aligns with performance measures 2020.XXX.*
- *We anticipate seeing an improvement in the quality and quantity of analytic production and responses to requests for information as a direct result of the funding of this project.*

The funding itemization for a fusion center project should include the amount and percent of each relevant solution area. As an example:

<b><i>Solution Area and Amount of Proposed Funding</i></b>	<b><i>Percent of Proposed Funding</i></b>
<i>Planning:</i> \$10,000.00	2%
<i>Organization:</i> \$200,000	48%
<i>Equipment:</i> \$200,000	48%
<i>Training:</i> \$10,000	2%
<i>Exercises:</i> \$0	0%
<b><i>Total:</i></b> \$420,000	<b>100%</b>

### ***Completing IJs in the Grant Reporting Tool (GRT) (SHSP and UASI)***

In the Related Documents section of the [Grants.gov](#) posting, applicants can find the IJ template and instructions for collecting the required information for investments and projects. Additionally, applicants should utilize the Project Worksheet located in [Grants.gov](#) posting to assemble the information required for each project, which will facilitate the input of that information into the GRT.

### ***Development of Concept of Operations for OPSG***

As part of the FY 2020 OPSG application process, each eligible local unit of government at the county or Federally recognized tribal government level must develop a strategic plan called a Concept of Operations (CONOP)/Application, which is a formal proposal of action to address a specific situation and forms the basis for Operations Orders, in coordination with state and Federal law enforcement agencies, to include, but not limited to CBP/USBP. CONOPs that are developed at the county level should be inclusive of city, county, tribal, and other local law enforcement agencies that are eligible to participate in OPSG operational activities, and the CONOP/Application should describe participating agencies in the Executive Summary.

CONOP/Application details should include the names of the agencies, points of contact, and individual funding requests. All CONOPs/Applications must be developed in collaboration with

the local USBP sector office, the SAA and the local unit of government. Requests for funding in CONOPs/Applications must be based on risks and the operational enforcement support requirements of its corresponding USBP Sector, as well as the national priorities identified below. USBP Sector offices will forward the CONOPs to USBP Headquarters for vetting and coordination. Applicants will forward corresponding OPSG Applications to the SAA for submission to FEMA. USBP Headquarters will reconcile all submitted CONOPs with the OPSG Applications. FEMA will review and evaluate all CONOPs and OPSG Applications and funding will be allocated based on the review and selection criteria identified in this NOFO.

**OPSG Applicants will be required to clearly articulate and identify how the CONOPs will address the national priorities identified below.**

### **Information Sharing and Cooperation**

Effective border security operations rely on timely information sharing and actionable intelligence to accurately assess and prevent threats against the United States. Accordingly, DHS works diligently to enhance intelligence collection, integration, analysis, and information sharing capabilities to ensure partners, stakeholders, and senior leaders receive actionable intelligence and information necessary to inform their decisions and operations. A critical and statutorily charged mission of DHS is to deliver intelligence and information to federal, state, local, and tribal governments and private sector partners. Cooperation and information sharing among state, federal, and local partners across all areas of the homeland security enterprise, including counterterrorism, cybersecurity, border security, immigration enforcement, and other areas is critical to homeland security operations and the prevention of, preparation for, protection against, and responding to acts of terrorism.

Given the importance of information sharing and collaboration to effective homeland security solutions, the CONOP must be in support of the recipient's efforts to enhance information sharing and cooperation with DHS and other federal agencies. Applicants must justify persuasively how they will contribute to the information sharing and collaboration purposes of the OPSG program and a culture of national preparedness, including how they will identify, address, and overcome any existing laws, policies, and practices that prevent information sharing. Additional resources and information regarding collaboration and information sharing are available through the Department's [Office of Intelligence and Analysis](#).

### **Emerging Threats**

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and non-state actors are aggressively working to develop, acquire, and modernize WMDs that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMDs than ever before. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities of threat actors to acquire and use these capabilities against the United States and its interests.

Given the increased risk of emerging threats, the CONOP must be in support of the recipient's efforts to address emerging threats. Additional resources and information regarding emerging threats are available through the [Countering Weapons of Mass Destruction Office](#) and the [Cybersecurity and Infrastructure Security Agency](#).

## **11. 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/2017/11/SPOC-Feb.-2018.pdf>.

## **12. Funding Restrictions**

Federal funds made available through this award may be used for the purpose set forth in this award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any 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. See the [Preparedness Grants Manual](#) for more information on funding restrictions.

## **13. Environmental Planning and Historic Preservation (EHP) Compliance**

See the [Preparedness Grants Manual](#) for information on EHP Compliance.

## **14. Emergency Communications Investments**

If an entity uses HSGP funding to support emergency communications investments, the following requirements shall apply to all such grant-funded communications investments in support of the emergency communications priorities and recognized best practices:

- Applicants must describe in the investment how proposed communications investments align to needs identified in their SCIP. Effective project alignment will require advance coordination with the SWIC and consultation with governing bodies such as the SIGB or Statewide Interoperability Executive Committee (SIEC), as they serve as the primary steering group for the statewide interoperability strategy. Additionally, recipients should consult subject matter experts serving on governance bodies, such as broadband experts, chief information officers, representatives from utilities, or legal and financial experts, when developing proposals.
- The signatory authority for the SAA must certify in writing to DHS/FEMA their compliance with the *SAFECOM Guidance*. The certification letter should be coordinated with the SWIC for each state and must be uploaded to [ND Grants](#) at the time of the first Program Performance Report (PPR) submission.
- All states and territories must designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government, to include establishing statewide plans, policies, and procedures, and coordinating decisions on communications investments funded through Federal grants. Note that the designated full-time SWIC may also be the state's or territory's cybersecurity point of contact. SWIC status information will be maintained by the DHS Office of Emergency Communications and will be verified by FEMA GPD through programmatic monitoring activities.
- By the period of performance end date, all states and territories must update the SCIP, with a focus on communications resilience/continuity, to include assessment and

mitigation of all potential risks identified in the SCIP: natural disasters, accidental damage (human failures), intentional damage (sabotage, terrorism), cybersecurity, etc. Following the initial update, the SCIP should be updated on an annual basis. SCIP status information will be maintained by the DHS Office of Emergency Communications and will be verified by FEMA GPD through programmatic monitoring activities.

All states and territories must test their emergency communications capabilities and procedures (as outlined in their operational communications plans) in conjunction with regularly planned exercises (separate/addition emergency communications exercises are not required) and must submit an After Action Report/Improvement Plan (AAR/IP) to the Homeland Security Exercise and Evaluation Program's (HSEEP) electronic message inbox at [hseep@fema.gov](mailto:hseep@fema.gov) within 90 days of exercise completion. Exercises should be used to both demonstrate and validate skills learned in training and to identify gaps in capabilities. Resilience and continuity of communications should be tested during training and exercises to the greatest extent possible. Further, exercises should include participants from multiple jurisdictions, disciplines, and levels of government and include emergency management, emergency medical services, law enforcement, interoperability coordinators, public health officials, hospital officials, officials from colleges and universities, and other disciplines and private sector entities, as appropriate. Findings from exercises should be used to update programs to address gaps in emergency communications as well as emerging technologies, policies, and partners. Recipients are encouraged to increase awareness and availability of emergency communications exercise opportunities across all levels of government.

States, territories, and other eligible grant recipients are advised that HSGP funding may be used to support communications planning (including the cost of hiring a SWIC, participation in governance bodies and requirements delineated [above](#)), training, exercises, and equipment costs. Costs for transitioning to the FirstNet network may also be eligible. More information regarding FirstNet can be found in the [Preparedness Grants Manual](#).

## **15. Detailed Budget**

Applicants must provide budget summary worksheets for all funds requested at the time of application. The budget summary worksheets must be complete, reasonable, and cost-effective in relation to the proposed project and should provide the basis of computation of all project-related costs (including management and administrative costs) and any appropriate narrative. FEMA must be able to thoroughly evaluate the projects being submitted based on the information provided. FEMA must be able to determine how much funding is being used by the direct recipient for projects carried out by the direct recipient and how much funding is being passed through to sub-recipients for each sub-program (UASI, SHSP, OPSG). Consequently, applicants must provide an appropriate level of detail within the budget summary worksheets to clarify what will be purchased and spent. Sample budget summary worksheets are available on the grants.gov posting for the HSGP in the Related Documents tab and may be used as a guide to assist applicants in the preparation of budgets and budget narratives.

## **16. Funds Transfer Restriction**

The recipient is prohibited from transferring funds between programs (includes the SHSP, the UASI, and OPSG). Recipients can submit an investment/project where funds come from multiple funding sources (e.g., the SHSP and UASI), however, recipients are not allowed to

divert funding from one program to another due to the risk-based funding allocations, which were made at the discretion of DHS/FEMA.

## **17. Pre-Award Costs**

Pre-award costs are allowable only with the prior written approval of DHS/FEMA and as included in the award agreement. To request pre-award costs, a written request must be included with the application, signed by the Authorized 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.

## **18. Cost Principles**

Costs charged to this award must be consistent with the Cost Principles for Federal Awards located at 2 C.F.R. Part 200, Subpart E. For more information on 2 C.F.R. Part 200, please refer to FEMA GPD Information Bulletin 400, [FEMA's Implementation of 2 C.F.R. Part 200, the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards](#) (“Super Circular” or “Omni Circular”).

## **19. Direct Costs**

### **a. Planning**

Planning costs are allowed under this program.

### **b. Organization**

Organization costs are allowed under this program.

### **c. Equipment**

Equipment costs are allowed under this program.

### **d. Training**

Training costs are allowed under this program.

### **e. Exercises**

Exercise costs are allowed under this program.

### **f. Personnel**

Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable HSGP planning, organization, training, exercise, and equipment activities. Under OPSG, overtime costs are allowable only in so far as they meet the intent of the program. All recipients and subrecipients of HSGP funds, including SHSP, UASI, and OPSG allocations, may not use more than 50 percent of their awards to pay for personnel activities unless a waiver is approved by FEMA. For more information on the 50 percent personnel cap, please see FEMA Information Bulletin (IB) 421, Clarification on the *Personnel Reimbursement for Intelligence Cooperation and Enhancement of Homeland Security Act of 2008* (Public Law 110-412) – the PRICE Act.

### **g. Operational Overtime**

Operational overtime costs are allowed under this program. Prior to use of funds for operational overtime, recipients must receive approval from DHS/FEMA.

**h. Travel**

Domestic travel costs are allowed under this program, as provided for in this NOFO. International travel is not an allowable cost under this program unless approved in advance by DHS/FEMA.

**i. Construction and Renovation**

Construction and renovation costs to achieve capability targets related to preventing, preparing for, protecting against, or responding to acts of terrorism are allowed under this program. For construction and renovation costs to be allowed, they must be specifically approved by DHS/FEMA in writing prior to the use of any program funds. Applicants must use the EHP approval process. Limits on the total amount of grant funding that may be used for construction or renovation may apply. Additionally, recipients are required to submit [Standard Form 424C](#).

**j. Maintenance and Sustainment**

Maintenance- and sustainment-related costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees, are allowable as described in FP 205-402-125-1, Maintenance Contracts and Warranty Coverage Funded by Preparedness Grants Policy (<http://www.fema.gov/media-library/assets/documents/32474>).

**k. Management and Administration (M&A) Costs**

Management and administration (M&A) activities are those directly relating to the management and administration of HSGP funds, such as financial management and monitoring. A maximum of up to five percent of HSGP funds awarded may be retained by the state, and any funds retained are to be used solely for M&A purposes associated with the HSGP award.

Subrecipients may also retain a maximum of up to five percent of the funding passed through by the state solely for M&A purposes associated with the HSGP award.

Recipients or subrecipients may apply or credit M&A funding toward the recipient's requirement to allocate funding toward the four national priority areas. For example, if a recipient spends \$5,000 to manage or administer its funding dedicated toward its enhancing cybersecurity investment, the recipient may credit that funding toward its requirement to allocate at least 5 percent of its award to enhancing cybersecurity.

A state's HSGP funds for M&A calculation purposes includes the total of its SHSP, UASI, and OPSG awards. While the SAA may retain up to five percent of this total for M&A, the state must still ensure that all subrecipient award amounts meet the mandatory minimum pass-through requirements that are applicable to each HSGP program. To meet this requirement, the percentage of SHSP and UASI funds passed through to local or tribal jurisdictions must be based on the state's total HSGP award prior to withholding any M&A.

In retaining these funds, states may retain a maximum of 2.5 percent of the OPSG allocation, which must be withheld from the pass-through to each subrecipient county or tribe in an equal percentage. The SAA may also retain additional funding from its SHSP award to manage and administer the OPSG award, but that additional amount is also capped at an amount equal to 2.5 percent of the OPSG award. Examples applying this principle:

**SAA 1:**

SHSP: \$1,000,000  
OPSG: \$2,500,000  
UASI: \$2,500,000

M&A Maximum: \$300,000 (5 percent of \$6,000,000)

Maximum M&A for SHSP = \$50,000

Maximum M&A for OPSG = \$125,000. Of that amount, \$62,500 (2.5 percent) may be retained from the OPSG allocation, and the other \$62,500 would come from the SHSP allocation. Any amount used to manage and administer OPSG that is charged to SHSP may be above and beyond the \$50,000 available to manage the SHSP allocation.

**SAA 2:**

SHSP: \$3,500,000  
OPSG: \$1,000,000

M&A Maximum: \$225,000 (5 percent of \$4,500,000)

Maximum M&A for SHSP: \$175,000

Maximum M&A for OPSG = \$50,000. Of that amount, \$25,000 (2.5 percent) may be retained from the OPSG allocation, and the other \$25,000 would come from the SHSP allocation. Any amount used to manage and administer OPSG that is charged to SHSP may be above and beyond the \$175,000 available to manage the SHSP allocation.

Please note, [Information Bulletin \(IB\) 365: Management and Administration Costs in the Homeland Security](#) and DHS/FEMA Policy 207-087-1, which can be found at [https://www.fema.gov/sites/default/files/2020-08/fema\\_clarification-allowable-m-a-costs-under-opsg.pdf?id=7837](https://www.fema.gov/sites/default/files/2020-08/fema_clarification-allowable-m-a-costs-under-opsg.pdf?id=7837), **do not apply to awards made in FY 2020 under this NOFO.** The IB and Policy remain in effect for all previous awards.

**L. Critical Emergency Supplies**

Critical emergency supplies are allowed under this program.

**M. Secure Identification**

Secure Identification costs are allowed under this program.

**N. Indirect (Facilities & 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 as discussed above.

**O. General Purpose Equipment**

HSGP allows expenditures on general purpose equipment if it aligns to and supports one or more core capabilities identified in the Goal and has a nexus to terrorism preparedness. General purpose equipment, like all equipment funded under the HSGP, must be sharable through the

Emergency Management Assistance Compact (EMAC)<sup>3</sup> and allowable under 6 U.S.C. § 609, and any other applicable provision of the *Homeland Security Act of 2002*, as amended. Examples of such general-purpose equipment may include:

- Law enforcement vehicles;
- Emergency medical services (EMS) equipment and vehicles;
- Fire service equipment and vehicles, to include hose, pump accessories, and foam concentrate for specialized chemical, biological, radiological, nuclear, and explosives (CBRNE) response;
- Interoperability of data systems, such as computer aided dispatch (CAD) and record management systems (RMS); and
- Office equipment for staff<sup>4</sup> engaged in homeland security program activity.

Equipment allowability is based on the [Authorized Equipment List \(AEL\)](#) but exceptions may be considered on a case-by-case basis if (1) the equipment identified to be purchased directly maps to a core capability contained within the Goal, and (2) the equipment's purpose (when operational) falls under the permitted use of funds in accordance with 6 U.S.C. § 609, and any other applicable provision of the *Homeland Security Act of 2002*, as amended.

## P. Allowable Cost Matrix

The following matrix provides allowable cost activities that fall under each of the cost categories noted above. Recipients and subrecipients must follow all applicable requirements in 2 C.F.R. Part 200 (*Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*). Funds under HSGP may be used to cover the costs for evaluating the impact of these grants on the state or urban area's core capabilities and capability gaps. This list is not exhaustive, therefore, if there are any questions regarding allowable costs, please contact the appropriate HQ GPD Program Analyst. For additional information on allowable costs, see the [Preparedness Grants Manual](#).

Allowable Program Activities	SHSP	UASI	OPSG
<b>Allowable Planning Costs</b>			
Developing hazard/threat-specific annexes	Y	Y	N
Developing and implementing homeland security support programs and adopting ongoing DHS/FEMA national initiatives	Y	Y	N
Developing related terrorism and other catastrophic event prevention activities	Y	Y	N
Developing and enhancing plans and protocols	Y	Y	N
Developing or conducting assessments	Y	Y	N
Hiring of full- or part-time staff or contract/consultants to assist with planning activities	Y	Y	N
Materials required to conduct planning activities	Y	Y	N
Travel/per diem related to planning activities	Y	Y	Y
Overtime and backfill costs (in accordance with operational Cost Guidance)	Y	Y	Y
Issuance of WHTI-compliant Tribal identification cards	Y	N	N
Activities to achieve planning inclusive of people with disabilities and others with access and functional needs and limited English proficiency.	Y	Y	N

<sup>3</sup> Except for American Samoa and the Commonwealth of the Northern Mariana Islands, which are not required to belong to EMAC at this time.

<sup>4</sup> This applies to all homeland security personnel and is not limited to management and administration staff, and costs are to be captured outside the cap on management and administration costs

Allowable Program Activities	SHSP	UASI	OPSG
Coordination with Citizen Corps Councils for public information/education and development of volunteer programs	Y	Y	N
Update governance structures and processes and plans for emergency communications	Y	Y	N
Development, and review and revision of continuity of operations plans	Y	Y	N
Development, and review and revision of the THIRA/SPR continuity of operations plans	Y	Y	N
<b>Allowable Organizational Activities</b>			
<b>Note:</b> 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.			
Program management	Y	Y	N
Development of whole community partnerships	Y	Y	N
Structures and mechanisms for information sharing between the public and private sector	Y	Y	N
Implementing models, programs, and workforce enhancement initiatives	Y	Y	N
Tools, resources, and activities that facilitate shared situational awareness between the public and private sectors	Y	Y	N
Operational support	Y	Y	N
Utilization of standardized resource management concepts	Y	Y	N
Responding to an increase in the threat level under the National Terrorism Advisory System (NTAS), or needs in resulting from a National Special Security Event	Y	Y	N
Reimbursement for select operational expenses associated with increased security measures at critical infrastructure sites incurred (up to 50 percent of the allocation)	Y	Y	Y
Overtime for information, investigative, and intelligence sharing activities (up to 50 percent of the allocation)	Y	Y	Y
Hiring of new staff positions/contractors/consultants for participation in information/intelligence analysis and sharing groups or fusion center activities (up to 50 percent of the allocation).	Y	Y	Y
<b>Allowable Equipment Categories</b>			
Personal Protective Equipment	Y	Y	Y
<b>Allowable Equipment Categories</b>			
Explosive Device Mitigation and Remediation Equipment	Y	Y	N
CBRNE Operational Search and Rescue Equipment	Y	Y	N
Information Technology	Y	Y	Y
Cybersecurity Enhancement Equipment	Y	Y	N
Interoperable Communications Equipment	Y	Y	Y
Detection	Y	Y	Y
Decontamination	Y	Y	N
Medical countermeasures	Y	Y	Y
Power (e.g., generators, batteries, power cells)	Y	Y	Y
CBRNE Reference Materials	Y	Y	N
CBRNE Incident Response Vehicles	Y	Y	N
Terrorism Incident Prevention Equipment	Y	Y	Y
Physical Security Enhancement Equipment	Y	Y	Y
Inspection and Screening Systems	Y	Y	Y
Animal Care and Foreign Animal Disease	Y	Y	N
CBRNE Prevention and Response Watercraft	Y	Y	N
CBRNE Prevention and Response Unmanned Aircraft	Y	Y	N
CBRNE Aviation Equipment	Y	Y	N
CBRNE Logistical Support Equipment	Y	Y	N
Intervention Equipment (e.g., tactical entry, crime scene processing)	Y	Y	Y
Critical emergency supplies	Y	Y	N
Vehicle acquisition, lease, and rental	N	N	Y
Other Authorized Equipment	Y	Y	Y

Allowable Program Activities	SHSP	UASI	OPSG
<b>Allowable Training Costs</b>			
Overtime and backfill for emergency preparedness and response personnel attending DHS/FEMA-sponsored and approved training classes	Y	Y	N
Overtime and backfill expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA training	Y	Y	N
Training workshops and conferences	Y	Y	Y
Activities to achieve training inclusive of people with disabilities and others with access and functional needs and limited English proficiency	Y	Y	N
Full- or part-time staff or contractors/consultants	Y	Y	Y
Travel	Y	Y	Y
Supplies	Y	Y	N
Instructor certification/re-certification	Y	Y	N
Coordination with Citizen Corps Councils in conducting training exercises	Y	Y	N
Interoperable communications training	Y	Y	N
Activities to achieve planning inclusive of people with limited English proficiency	Y	Y	N
Immigration enforcement training	Y	Y	Y
<b>Allowable Exercise Related Costs</b>			
Design, Develop, Conduct, and Evaluate an Exercise	Y	Y	N
Full- or part-time staff or contractors/consultants	Y	Y	N
Overtime and backfill costs, including expenses for part-time and volunteer emergency response personnel participating in DHS/FEMA exercises	Y	Y	N
Implementation of HSEEP	Y	Y	N
Activities to achieve exercises inclusive of people with disabilities and others with access and functional needs	Y	Y	N
Travel	Y	Y	N
Supplies	Y	Y	N
Interoperable communications exercises	Y	Y	N
<b>Allowable Exercise Related Costs</b>			
Activities to achieve planning inclusive of people with limited English proficiency	Y	Y	N
<b>Allowable Management &amp; Administrative Costs</b>			
Hiring of full- or part-time staff or contractors/consultants to assist with the management of the respective grant program, application requirements, and compliance with reporting and data collection requirements	Y	Y	Y
Development of operating plans for information collection and processing necessary to respond to DHS/FEMA data calls	Y	Y	Y
Overtime and backfill costs	Y	Y	Y
Travel	Y	Y	Y
Meeting related expenses	Y	Y	Y
Authorized office equipment	Y	Y	Y
Recurring expenses such as those associated with cell phones and faxes during the PoP of the grant program	Y	Y	N
Leasing or renting of space for newly hired personnel during the PoP of the grant Program	Y	Y	N
<b>Law Enforcement Terrorism Prevention Activities (LETPA) Costs</b>			
Integration and interoperability of systems and data, such as CAD and RMS, to facilitate the collection,	Y	Y	N
Maturation and enhancement of designated state and major Urban Area fusion centers	Y	Y	N
Coordination between fusion centers and other analytical and investigative efforts	Y	Y	N

Allowable Program Activities	SHSP	UASI	OPSG
Implementation and maintenance of the Nationwide SAR Initiative	Y	Y	N
Implementation of the "If You See Something, Say Something®" campaign	Y	Y	N
Increase physical security, through law enforcement personnel and other protective measures, by implementing preventive and protective measures at critical	Y	Y	N
Building and sustaining preventive radiological and nuclear detection capabilities	Y	Y	N

## **E. Application Review Information**

### **1. Application Evaluation Criteria**

#### **a. Programmatic Criteria**

##### **Allocations**

###### **Risk Methodology and Effectiveness Review**

The risk methodology and effectiveness review first determine the relative risk of terrorism faced by a given area considering the potential risk of terrorism to people, critical infrastructure, and economic security. The analysis includes, but is not limited to, threats from violent domestic extremists, international terrorist groups, and individuals inspired by terrorists abroad. See the [Preparedness Grants Manual](#) and Application Evaluation Criteria for additional information on risk methodology and effectiveness review.

The second part of the risk methodology and effectiveness review determines whether the proposed project is clear, logical, and reasonable to address the priority area of interest and contribute to a culture of national preparedness. This part considers factors such as how well the project is described and how well the project addresses the objectives and strategies of the priority area.

Risk and effectiveness will be given equal consideration in determining final award amounts.

NOTE: The THIRA/SPR process is separate from the risk methodology and effectiveness review, and its results do not affect grant allocations.

##### **Evaluation Criteria**

FEMA will evaluate the FY 2020 HSGP applications for completeness, adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments. FEMA's review will include verification that each IJ or project:

- Meets the national priority required spend percentages.
- Aligns with at least one core capability identified in the Goal;
- Demonstrates how investments support closing capability gaps or sustaining capabilities identified in the THIRA/SPR process; and
- Supports a NIMS-typed resource and whether those assets are deployable/shareable to support emergency or disaster operations per existing EMAC agreements.

In addition to the above, FEMA will determine whether the proposed approach is clear, logical, and reasonable to address the priority areas of interest and contribute to a culture of national preparedness. This part considers factors such as the objectives and strategies proposed to address the priority area, how the objectives and strategies overcome legal, political, or practical obstacles to reduce overall risk, the process and criteria to select additional relevant projects, and the approach to monitor awards to satisfy the funding percentage allocations. Effectiveness will be evaluated prior to award and may impact the final overall award amount. To that end, IJs should include:

- How the proposed investment addresses the national priority;
- An explanation of how the proposed projects were selected and will achieve objectives and strategies to build or sustain the core capability gaps identified in the SPR, including expected long-term impact where applicable;
- A summary of laws, policies and practices that can be enhanced, eliminated, or otherwise changed in order to achieve the goals of the project and foster a culture of national preparedness;
- A summary of the collaboration efforts to prevent, prepare for, protect against, and respond to acts of terrorism as well as anticipated outcomes of the project.

For FY 2020 HSGP applications, effectiveness will be evaluated based on the following five factors:

- Investment Strategy (30%): Proposals will be evaluated based on the quality and extent to which applicants describe an effective strategy that demonstrates that proposed projects support the program objective of preventing, preparing for, protecting against, and responding to acts of terrorism, to meet its target capabilities, and otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation.
- Budget (10%): Proposals will be evaluated based on the extent to which applicants describe a budget plan for each investment demonstrating how the applicant will maximize cost effectiveness of grant expenditures.
- Impact/Outcomes (30%): Proposals will be evaluated on how this investment helps the jurisdiction close capability gaps identified in its Stakeholder Preparedness Review and addresses national priorities outlined in the FY 2020 NOFO. Further, proposals will be evaluated on their identification and estimated improvement of core capability(ies), the associated standardized target(s) that align with their proposed investment, and the ways in which the applicant will measure and/or evaluate improvement.
- Collaboration (30%): Proposals will be evaluated based on the degree to which the proposal adequately details how the recipient will use investments and other means to overcome existing logistical, technological, legal, policy, and other impediments to collaborating, networking, sharing information, cooperating, and fostering a culture of national preparedness with federal, state, tribal, and local governments, as well as other regional and nonprofit partners in efforts to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, support the national security mission of DHS and other federal agencies, and to otherwise reduce the overall risk to the high-risk urban area, the State, or the Nation. In evaluating applicants under this factor FEMA will consider the information provided by the applicant and may also consider relevant information from other sources.
- Past Performance (additional consideration): Proposals will be evaluated based on the

applicants demonstrated capability to execute the proposed investments. In evaluating applicants under this factor FEMA will consider the information provided by the applicant and may also consider relevant information from other sources.

Recipients are 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.

#### **Review and Selection Process (SHSP and UASI)**

To ensure the effectiveness of proposed investments and projects, all applications will undergo a Federal review as described herein. The Federal review will be conducted by DHS and FEMA. IJs will be reviewed at both the investment and project level. Results of the effectiveness analysis may result in a recipient receiving a reduced grant award.

Cybersecurity investments will be reviewed by DHS/FEMA, CISA, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

Soft Targets/Crowded Places investments will be reviewed by DHS/FEMA, CISA, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

Information Sharing and Cooperation Investments will be reviewed by DHS/FEMA, DHS Intelligence and Analysis, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

As part of the above, Fusion center projects will be reviewed by DHS/FEMA for compliance with HSGP NOFO requirements to prioritize the alignment of requests with results from the annual Fusion Center Assessment Program. If a fusion center investment does not meet the requirements, a Fusion Center Addendum must be completed and submitted for review and approval prior to expending funds allocated to fusion center activities.

Emerging threats investments will be reviewed by DHS/FEMA, DHS Countering Weapons of Mass Destruction Office, and other DHS components as appropriate, for compliance with purposes and requirements of the priority investment area. Proposed investments will be reviewed for effectiveness using the criteria set forth in this NOFO.

All other proposed investments not associated with a required investment justification will undergo a Federal review by DHS/FEMA to verify compliance with all administrative and eligibility criteria identified in the NOFO.

#### **Review and Selection Process (OPSG)**

Applications will be reviewed by the SAA and USBP for completeness and adherence to programmatic guidelines and evaluated for anticipated feasibility, need, and impact of the

Operations Orders. For more information on Operations Orders and other requirements of OPSG, see the [Preparedness Grants Manual](#).

DHS/FEMA will verify compliance with all administrative and eligibility criteria identified in the NOFO and required submission of Operations Orders and Inventory of Operations Orders by the established due dates. DHS/FEMA and USBP will use the results of both the risk analysis and the Federal review by DHS/FEMA to make recommendations for funding to the Secretary of Homeland Security.

FY 2020 OPSG funds will be allocated competitively based on risk-based prioritization using the OPSG Risk Assessment described above. Final funding allocations are determined by the Secretary, who may consider information and input from various law enforcement offices or subject-matter experts within the Department. Factors considered include, but are not limited to, threat, vulnerability, miles of the border, and other border-specific law enforcement intelligence, as well as the feasibility of FY 2020 Operations Orders to designated localities within border states and territories.

**b. Financial Integrity Criteria**

Prior to making a Federal award, DHS/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. Application evaluation criteria may include the following risk-based considerations of the applicant:

- Financial stability;
- Quality of management systems and ability to meet management standards;
- History of performance in managing Federal awards;
- Reports and findings from audits; and
- Ability to effectively implement statutory, regulatory, or other requirements.

**c. Supplemental Financial Integrity Review**

Prior to making a Federal award where the anticipated Federal share of a Federal award will be greater than the simplified acquisition threshold, currently \$250,000 (*see* Section 805 of the National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 115-91, OMB Memorandum M-18-18 at <https://www.whitehouse.gov/wp-content/uploads/2018/06/M-18-18.pdf>; *see also* [FEMA GPD 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 also 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.

## **F. Federal Award Administration Information**

### **1. Notice of Award**

See the [Preparedness Grants Manual](#) for information on Notice of Award.

### **2. SHSP and UASI Pass-Through Requirements**

Awards made to the SAA for HSGP carry additional pass-through requirements. Pass-through is defined as an obligation on the part of the SAA to make funds available to local units of government, combinations of local units, tribal governments, or other specific groups or organizations. Four requirements must be met to pass-through grant funds:

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

#### **Timing and Amount**

The SAA must pass-through at least 80 percent of the funds awarded under the SHSP and UASI to local or tribal units of government within 45 calendar days of receipt of the funds. "Receipt of the funds" occurs either when the SAA accepts the award or 15 calendar days after the SAA receives notice of the award, whichever is earlier.

SAAs are sent notification of HSGP awards via the GPD's 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 days pass-through period will start on the date the SAA accepted the award. Should an SAA not accept the HSGP award within 15 calendar days of receiving notice of the award in the 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 days pass-through period. For example, an SAA may receive notice of the HSGP 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 HSGP 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.

#### **Other SHSP and UASI Pass-Through Requirements**

The signatory authority of the SAA must certify in writing to DHS/FEMA that pass-through requirements have been met. A letter of intent (or equivalent) to distribute funds is not considered sufficient. The pass-through requirement does not apply to SHSP awards made to the District of Columbia, Guam, American Samoa, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. The Commonwealth of Puerto Rico is required to comply with the pass-through requirement, and its SAA must also obligate at least 80 percent of the funds to local units of government within 45 calendar days of receipt of the funds.

Under SHSP, the SAA may retain more than 20 percent of funding for expenditures made by the state on behalf of the local unit(s) of government. This may occur only with the written consent of the local unit of government, specifying the amount of funds to be retained and the intended use of funds. States shall review their written consent agreements yearly and ensure that they are still valid. If a written consent agreement is already in place from previous fiscal years, DHS/FEMA will continue to recognize it for FY 2020, unless the written consent review indicates the local government is no longer in agreement. If modifications to the existing agreement are necessary, the SAA should contact their assigned FEMA HQ Program Analyst.

### **Additional OPSG Requirements**

The recipient is prohibited from obligating or expending funds provided through this award until each unique and specific county-level or equivalent Operational Order/Fragmentary Operations Order budget has been reviewed and approved through an official electronic mail notice issued by DHS/FEMA removing this special programmatic condition.

## **3. Administrative and National Policy Requirements**

See the [Preparedness Grants Manual](#) for information on Administrative and National Policy requirements.

## **4. Reporting**

See the [Preparedness Grants Manual](#) for information on reporting requirements, including federal financial reporting requirements, programmatic performance reporting requirements, and closeout reporting requirements.

### **Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Process**

See the [Preparedness Grants Manual](#) for information on the THIRA and SPR process.

### **Supplemental Information Reporting Systems**

In addition to ND Grants, the following information systems are used for the submission of required reports:

#### **Grant Reporting Tool (GRT)**

Information on the GRT can be found in the [Preparedness Grants Manual](#).

#### **Unified Reporting Tool (URT)**

See the [Preparedness Grants Manual](#) for information on the URT.

#### **Closeout Reporting Requirements**

See the [Preparedness Grants Manual](#) for information on closeout reporting requirements.

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

See the [Preparedness Grants Manual](#) for information on disclosing information.

## **5. Monitoring**

Per 2 C.F.R. § 200.336, DHS/FEMA through its authorized representatives, has the right, at all reasonable times, to make site visits to review project accomplishments and management control

systems to review project accomplishments and to provide any required technical assistance. During site visits, DHS/FEMA will review grant recipients' files related to the grant award. As part of any monitoring and program evaluation activities, grant recipients must permit DHS/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 DHS/FEMA requests for information relating to the grant program. See the [Preparedness Grants Manual](#) for additional information on monitoring.

## **G. DHS/FEMA Awarding Agency Contact Information**

### **1. Contact and Resource Information**

#### **Centralized Scheduling and Information Desk (CSID)**

CSID is a non-emergency comprehensive management and information resource developed by DHS/FEMA for grant stakeholders. CSID provides general information on all DHS/FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the Federal, state, and local levels. When necessary, recipients will be directed to a Federal point of contact who can answer specific programmatic questions or concerns. CSID can be reached by phone at (800) 368-6498 or by e-mail at [askcsid@fema.gov](mailto:askcsid@fema.gov), Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

#### **GPD Grant Operations Division**

GPD's Grant Operations Division Business Office provides support regarding financial matters and budgetary, technical assistance. Additional guidance and information can be obtained by contacting the FEMA Call Center at 866-927-5646 or via e-mail to [ASK-GMD@fema.gov](mailto:ASK-GMD@fema.gov).

#### **FEMA Regional Offices**

FEMA Regional Offices may also provide fiscal support, including pre- and post-award administration and technical assistance such as conducting cash analysis, financial monitoring, and audit resolution for the grant programs included in this solicitation. GPD will provide programmatic support and technical assistance. FEMA Regional Office contact information is available [here](#).

#### **GPD Environmental Planning and Historic Preservation (EHP)**

The DHS/FEMA GPD EHP Team provides guidance and information about the EHP review process to recipients and subrecipients. All inquiries and communications about GPD projects or the EHP review process, including the submittal of EHP review materials, should be sent to [gpdehpinfo@fema.dhs.gov](mailto:gpdehpinfo@fema.dhs.gov). EHP Technical Assistance, including the EHP Screening Form, can be found online at <https://www.fema.gov/grants/preparedness/preparedness-grants-ehp-compliance>.

### **2. Systems Information**

#### **Grants.gov**

For technical assistance with [Grants.gov](#), call the customer support hotline 24 hours per day, 7 days per week (except Federal holidays) at (800) 518-4726 or e-mail at [support@grants.gov](mailto:support@grants.gov).

#### **Non-Disaster (ND) Grants**

For technical assistance with the ND Grants system, please contact the ND Grants Helpdesk at

[ndgrants@fema.gov](mailto:ndgrants@fema.gov) or (800) 865-4076, Monday through Friday, 9:00 a.m. – 5:00 p.m. ET.

### **Payment and Reporting System (PARS)**

DHS/FEMA uses the [Payment and Reporting System \(PARS\)](#) for financial reporting, invoicing and tracking payments. DHS/FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, recipients must complete a Standard Form 119A, Direct Deposit Form.

## **H. Additional Information**

GPD has developed the [Preparedness Grants Manual](#) to guide applicants and recipients of grant funding on how to manage their grants and other resources. Recipients seeking guidance on policies and procedures for managing preparedness grants should reference the Manual for further information. Examples of information contained in the [Preparedness Grants Manual](#) include:

- Conflicts of Interest in the Administration of Federal Awards and Subawards;
- Extensions;
- Monitoring;
- Procurement Integrity; and
- Other Post-Award Requirements.

In response to recent disasters, FEMA has introduced a new lifelines 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. To learn more about lifelines, please refer to the [Preparedness Grants Manual](#), or visit <https://www.fema.gov/emergency-managers/national-preparedness/frameworks>.

Additionally, recipients can access 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.



***Cal OES***

**GOVERNOR'S OFFICE  
OF EMERGENCY SERVICES**

**Fiscal Year 2020  
Homeland Security Grant Program**

***California Supplement to the  
Federal Notice of Funding Opportunity***

December 2020

<b>SECTION 1—OVERVIEW.....</b>	<b>1</b>
Federal Program Announcement	
Information Bulletins	
Grant Management Memoranda	
Purpose of the California Supplement	
Eligible Subrecipients	
Tribal Allocations	
Subrecipient Allocations	
Supplanting	
Public/Private Organizations	
Debarred/Suspended Parties	
Key Changes to the FY 2020 HSGP	
<b>SECTION 2—FEDERAL CHANGES AND INITIATIVES .....</b>	<b>5</b>
FY 2020 National Priorities	
National Campaigns and Programs	
National Cybersecurity Review	
NIMS Implementation	
Law Enforcement Terrorism Prevention Activities	
Management and Administration	
Indirect Costs	
Organization Costs – Overtime	
Personnel Cap	
Equipment Typing/Identification and Use	
Equipment Maintenance/Sustainment	
Emergency Communications Projects	
Telecommunications Equipment and Services Prohibitions	
Small Unmanned Aircraft Systems	
Emergency Operations Plans	
Conflict of Interest	
<b>SECTION 3—STATE CHANGES AND INITIATIVES .....</b>	<b>13</b>
FY 2020 Investments	
California Homeland Security Strategy Goals	
State Initiative Funding	
“On Behalf Of”	
Regional Approach	
Public Alert and Warning	
<b>SECTION 4—REQUIRED STATE APPLICATION COMPONENTS.....</b>	<b>15</b>
Financial Management Forms Workbook	
Subrecipient Grants Management Assessment	
Application Attachments	
Standard Assurances	

Operational Areas Only	
Urban Areas Only	
Fusion Centers Only	
State Agencies and Tribes Only	
<b>SECTION 5—THE STATE APPLICATION PROCESS .....</b>	<b>20</b>
Application Submission	
Late or Incomplete Application	
HSGP Contact Information	
Subaward Approval	
<b>SECTION 6—POST AWARD REQUIREMENTS .....</b>	<b>22</b>
Payment Request Process	
Advances and Interest Earned on Advances	
Semi-Annual Drawdown Requirements	
Modifications	
Training	
Exercises, Improvement Plans, and After Action Reporting	
Procurement Standards and Written Procedures	
Procurement Thresholds	
Procurement Documentation	
Noncompetitive Procurement	
Performance Bond	
Environmental Planning and Historic Preservation	
Construction and Renovation	
Inventory Control and Property Management	
Equipment Disposition	
Performance Reporting	
Extension Requests	
Progress Reports on Grant Extensions	
Monitoring	
Failure to Submit Required Reports	
Suspension/Termination	
Closeout	
Records Retention	
<b>ATTACHMENTS</b>	
A – FY 2020 HSGP Allocations	
B – FY 2020 HSGP Timeline	
C – FY 2020 HSGP Application Checklist	

**Federal Program Announcement**

In April 2020, the U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) issued the Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP), [Notice of Funding Opportunity](#) (NOFO) and the [FEMA Preparedness Grants Manual](#).

Subrecipients must follow the programmatic requirements in the NOFO, FEMA Preparedness Grants Manual, and the applicable provisions of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards located in [Title 2, Code of Federal Regulations \(C.F.R.\), Part 200](#).

**Information Bulletins**

DHS issues [Information Bulletins](#) (IBs) to provide updates, clarification, and new requirements throughout the life of the grant.

**Grant Management Memoranda**

Cal OES issues [Grant Management Memoranda](#) (GMMs) which provide additional information and requirements regarding HSGP funds.

**Purpose of the California Supplement**

The FY 2020 HSGP California Supplement to the NOFO (State Supplement) is intended to complement, rather than replace, the NOFO and the FEMA [Preparedness Grants Manual](#). It is recommended that Applicants thoroughly read the NOFO and the Preparedness Grants Manual before referring to the State Supplement. The State Supplement will emphasize differences between the FY 2019 and FY 2020 HSGP and highlight additional California policies and requirements applicable to FY 2020 HSGP.

**Eligible Subrecipients**

Eligible Applicants, referred to as Subrecipients, include Counties/Operational Areas (OAs), Urban Areas (UAs), State Agencies (SAs), Departments, Commissions, and Boards who have or can obtain appropriate state Department of Finance budget authority for awarded funds, and federally-recognized tribes located in California.

**Tribal Allocations**

The NOFO strongly encourages Cal OES to provide HSGP funds directly to tribes in California. To implement this requirement, a special Request for Proposal will be issued to California's federally-recognized tribes. All Subrecipients are encouraged to coordinate with tribal governments to ensure that tribal needs are considered in their grant applications.

---

<b>Subrecipient Allocations</b>	FY 2020 HSGP Subrecipient allocations are included in Attachment A.
<b>Supplanting</b>	Grant funds must be used to supplement existing funds, not replace (supplant) funds that have been appropriated for the same purpose. Subrecipients may be required to provide supporting documentation that certifies a reduction in non-federal resources that occurred for reasons other than the receipt or expected receipt of federal funds. Supplanting will result in the disallowance of the activity(ies) associated with this improper use of the federal grant funds.
<b>Public/Private Organizations</b>	Subrecipients may contract with other public or private organizations to perform eligible activities on approved HSGP projects.
<b>Debarred/ Suspended Parties</b>	Subrecipients must not make or permit any award (subaward or contract) at any tier, to any party, that is debarred, suspended, or otherwise excluded from, or ineligible for, participation in federal assistance programs.
	Subrecipients must obtain documentation of eligibility before making any subaward or contract using HSGP funds and must be prepared to present supporting documentation to monitors/auditors.
	Before entering into a Grant Subaward, the Subrecipient must notify Cal OES if it knows if any of the principals under the subaward fall under one or more of the four criteria listed at <a href="#">2 C.F.R. § 180.335</a> . The rule also applies to Subrecipients who pass-through funding to other local entities.
	If at any time after accepting a subaward, Subrecipients learn that any of its principals fall under one or more of the criteria listed at <a href="#">2 C.F.R. § 180.335</a> , immediate written notice must be provided to Cal OES and all grant activities halted until further instructions are received from Cal OES. The rule also applies to subawards passed through by Subrecipients to local entities.
<b>Key Changes to the FY 2020 HSGP</b>	<ul style="list-style-type: none"><li>• A minimum of 5% of total awarded funds must be allocated towards each of the four national priority areas, each with their own designated Investment Justification.</li></ul>

**Key Changes to  
the FY 2020  
HSGP (cont.)**

- Enhancing cybersecurity (including election security);
- Enhancing the protection of soft targets/crowded places (including election security);
- Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS; and
- Addressing emerging threats (e.g., transnational criminal organizations, weapons of mass destruction [WMDs], unmanned aerial systems [UASs], etc.).
- Governing Body Resolutions (GBR) may be valid for up to three years and can be used for multiple grant programs, provided certain criteria is met.
- Effective August 13, 2020, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits FEMA Recipients and Subrecipients (including their contractors and subcontractors) from obligating or expending federal funds on certain telecommunications products and contracting with certain entities for national security reasons.

### FY 2020 National Priorities

DHS/FEMA annually publishes the [National Preparedness Report](#) (NPR) to report national progress in building, sustaining, and delivering the core capabilities outlined in the goal of a secure and resilient nation. This analysis provides a national perspective on critical preparedness trends for whole community partners to use to inform program priorities, allocate resources, and communicate with stakeholders about issues of concern.

HSGP Subrecipients are required to prioritize grant funding to demonstrate how investments support closing capability gaps or sustaining capabilities identified in the Threat Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR\_ process.

DHS/FEMA continually assess changes to the threat landscape to further the National Preparedness Goal (NPG) of a secure and resilient nation. The following are national priority areas for FY 2020:

- Enhancing cybersecurity (including election security);
- Enhancing the protection of soft targets/crowded places (including election security);
- Enhancing information and intelligence sharing and cooperation with federal agencies, including DHS; and
- Addressing emerging threats (e.g., transnational criminal organizations, WMDs, UASs, etc.).

Subrecipients are required to allocate 5% of their subaward towards projects that fall within each of the national priority areas, totaling 20% of their subaward. Both Enhancing Cybersecurity (IJ #3) and Enhancing the Protection of Soft Targets/Crowded Places (IJ #2) must each comprise of one election security project (no minimum allocation amount for election security projects).

National Priority projects will be reviewed for effectiveness by DHS/FEMA in the December 2020 BSIR and must be deemed effective prior to the obligation or expenditure of funds. Project costs incurred prior to DHS/FEMA project approval will not be allowable.

Projects may require additional information for DHS/FEMA to determine effectiveness of the project. In these cases, the project will remain on hold pending submission of the requested information and DHS/FEMA approval.

**FY 2020 National Priorities (cont.)**

Once a project is deemed effective by DHS/FEMA, any modification to the project requires DHS/FEMA approval.

Effectiveness will be evaluated based on the following five factors:

- **Investment Strategy (30%):** Proposals will be evaluated based on the quality and extent to which Applicants describe an effective strategy that demonstrates that proposed projects support the program objective of preventing, preparing for, protecting against, and responding to acts of terrorism, to meet its target capabilities, and otherwise reduce the overall risk to the high-risk urban area, the state, or the nation.
- **Budget (10%):** Proposals will be evaluated based on the extent to which Applicants describe a budget plan for each investment demonstrating how the Applicant will maximize cost effectiveness of grant expenditures.
- **Impact/Outcomes (30%):** Proposals will be evaluated on how this investment helps the jurisdiction close capability gaps identified in its Stakeholder Preparedness Review and addresses national priorities outlined in the FY 2020 NOFO. Further, proposals will be evaluated on their identification and estimated improvement of core capability(ies), the associated standardized target(s) that align with their proposed investment, and the ways in which the Applicant will measure and/or evaluate improvement.
- **Collaboration (30%):** Proposals will be evaluated based on the degree to which the proposal adequately details how the Recipient will use investments and other means to overcome existing logistical, technological, legal, policy, and other impediments to collaborating, networking, sharing information, cooperating, and fostering a culture of national preparedness with federal, state, tribal, and local governments, as well as other regional and nonprofit partners in efforts to prevent, prepare for, protect against, and respond to acts of terrorism, to meet its target capabilities, support the national security mission of DHS and other federal agencies, and to otherwise reduce the overall risk to the high-risk urban area, the state, or the nation. In evaluating Applicants under this factor, FEMA will consider the information provided by the Applicant and may also consider relevant information from other sources.

**FY 2020 National Priorities (cont.)**

- **Past Performance (additional consideration):** Proposals will be evaluated based on Applicant's demonstrated capability to execute the proposed investments. In evaluating Applicants under this factor, FEMA will consider the information provided by the Applicant and may also consider relevant information from other sources.

Subrecipients who are unable to meet the 5% requirement for each national priority area may submit a waiver request. Waiver requests for each priority area will be approved on a case-by-case basis and can only be approved after the State, as a whole, has met or exceeded the 5% national priority requirement for each area.

A detailed description of allowable investments for each national priority is included in the [FY 2020 HSGP NOFO \(Page 4-6\)](#).

**National Campaigns and Programs**

**Whole Community Preparedness** – Subrecipients 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, Subrecipients are encouraged to consider the needs of individuals with disabilities and limited English proficiency in the activities and projects funded by the grant.

Subrecipients should utilize established best practices for whole community inclusion and engage with stakeholders to advance individual and jurisdictional preparedness and resilience. In doing so, Subrecipients are encouraged to consider the necessities of all Californians in the activities and projects funded by the grant including individuals with access or functional needs, defined as:

Individuals with physical, developmental or intellectual disabilities, chronic conditions or injuries, or limited English proficiency; or, individuals who are older adults, children, low income, homeless, transportation disadvantaged, or pregnant.

**Active Shooter Preparedness** – DHS developed a comprehensive [Active Shooter Preparedness website](#), which strives 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. Subrecipients are encouraged to review the referenced active shooter resources and evaluate their preparedness needs.

**National Campaigns and Programs (cont.)**

**Soft Targets and Crowded Places** – States, territories, UAs, and public and private sector partners are encouraged to identify security gaps and build capabilities that address security needs and challenges related to protecting locations which are open to the public and to use resources to instill a culture of awareness, vigilance, and preparedness. For more information, please see DHS's [Hometown Security Program](#).

**Community Lifelines** – FEMA has a lifeline construct to enable the operational continuity of government and critical business essential to human health, safety, or economic security during and after a disaster. These lifelines enable a true unity of effort between government, non-governmental organizations, and the private sector, including infrastructure owners and operators. Additional information may be found at the [Community Lifelines Implementation Toolkit website](#).

**Strategic Framework for Countering Terrorism and Targeted Violence** – Terrorist organizations remain a core priority of DHS's counterterrorism efforts and DHS will continue to make substantial progress in the ability to detect, prevent, protect against, and mitigate the threats these groups pose. DHS 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.

**National Cybersecurity Review**

The [National Cybersecurity Review \(NCSR\)](#) is a required assessment for all Subrecipients of State Homeland Security Program (SHSP) and Urban Areas Security Initiative (UASI) funding to be completed between October and December 2020.

The NCSR is a no-cost, anonymous, and annual self-assessment designed to measure gaps and capabilities of state, local, tribal, territorial, nonprofit, and private sector agencies' cybersecurity programs.

The Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent should complete the NCSR. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment. Additional information may be found in [IB 439](#) and [429a](#).

### **NIMS Implementation**

Prior to the allocation of any federal preparedness awards in FY 2020, Subrecipients must ensure and maintain the adoption and implementation of the [National Incident Management System](#) (NIMS).

### **Law Enforcement Terrorism Prevention Activities**

A minimum of 25 percent of FY 2020 HSGP funds must be dedicated to Law Enforcement Terrorism Prevention Activities (LETPA). To leverage funds for LETPA, activities outlined in the National Prevention Framework and National Protection Framework are eligible for use of LETPA-focused funds. All other terrorism prevention activities proposed for funding under LETPA must be formally pre-approved by FEMA. Refer to [IB 412](#) for additional information.

### **Management and Administration**

The Management and Administration (M&A) allowance for Subrecipients is set at a maximum of 5% for FY 2020 HSGP.

### **Indirect Costs**

Indirect costs are allowable under the FY 2020 HSGP Grant Award. Subrecipients who claim indirect costs may do so, provided they use one of the following two methods:

1. Subrecipients with an indirect cost rate approved by their cognizant federal agency may claim indirect costs based on the established rate. Indirect costs claimed must be calculated using the base approved in the indirect cost negotiation agreement. A copy of the approved negotiation agreement is required at the time of application.
2. Subrecipients who have never received a negotiated indirect cost rate and receive *less than* \$35 million in *direct* federal funding per year may claim the 10 percent *de minimis* indirect cost rate based on Modified Total Direct Costs (MTDC) as described in [2 C.F.R. § 200.68](#) and Subpart E.

Indirect costs are *in addition to* the M&A allowance and must be included in the Grant Award application as a “Project” and reflected in the Financial Management Forms Workbook (FMFW) on the Indirect cost category ledger if being claimed under the award.

Indirect costs must be based on the claimed direct project costs, excluding equipment expenditures and other distorting items. Up to \$25,000 of each subaward may be included as a direct project cost when calculating indirect costs based on MTDC.

### **Indirect Costs (cont.)**

Indirect costs must be claimed no more than once annually, and only at the end of the Subrecipient's fiscal year. An exception to this rule applies if there is a mid-year change to the approved indirect cost rate; in this case, costs incurred to date must be claimed. At that time, a Grant Subaward Modification reflecting the rate change must also be submitted to Cal OES, along with a copy of the new indirect cost rate agreement.

### **Organization Costs - Overtime**

Operational overtime costs are allowable for increased security measures at critical infrastructure sites if associated with detecting, deterring, disrupting, and preventing acts of terrorism and other catastrophic events.

Pursuant to page A-17 of the [Preparedness Grants Manual](#), all operational overtime requests must clearly explain how the request meets the criteria of one or more of the categories listed in *Table 2: Authorized Operational Overtime Categories*.

Requests must address the threat environment as it relates to the event or activity requiring operational overtime support and explains how the overtime activity is responsive to the threat. Post-event operational overtime requests will only be considered on a case-by-case basis, where it is demonstrated exigent circumstances prevented submission of a request in advance of the event or activity. Requests for overtime costs must be submitted to Cal OES via the [Request for Operational Overtime Form](#) at the time of application, if the activity will occur within one year of the final application submission. All subsequent requests must be submitted at least 60 days in advance of the activity. **All operational overtime costs must be formally pre-approved in writing by DHS/FEMA.**

### **Personnel Cap**

Pursuant to [6 U.S.C. § 609\(b\)](#), SHSP and UASI funds may be used for personnel costs, totaling up to 50 percent of each fund source. A Subrecipient may request this requirement be waived by DHS/FEMA, via Cal OES. Requests for personnel cap waivers must be submitted separately for each fund source in writing to the Program Representative on official letterhead, with the following information:

**Personnel Cap  
(cont.)**

- Documentation explaining why the cap should be waived;
- Conditions under which the request is being submitted; and
- A budget and method of calculation of personnel costs both in percentages of the Grant Award and in total dollar amount (waivers must be calculated separately for SHSP and UASI, outlining salary, fringe benefits, and any M&A costs).

Subrecipient requests to exceed the personnel cap must be received by Cal OES at the time of application. Subaward modifications impacting the personnel cap will be reviewed on a case-by-case basis and may require the submittal of the above-mentioned information.

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

**Equipment  
Typing/  
Identification  
and Use**

Allowable HSGP equipment is listed on the [FEMA Authorized Equipment List \(AEL\)](#) website.

Subrecipients that allocate FY 2020 HSGP funds towards equipment are required to type and identify the capability associated with that equipment. The [FEMA Resource Typing Library Tool \(RTLT\)](#) can be used to help determine the type and capability.

Per FEMA policy, the purchase of weapons and weapon accessories are not allowed with HSGP funds. Special rules apply to pharmaceutical purchases, medical countermeasures, and critical emergency supplies; refer to page A-22 of the Preparedness Grants Manual for additional information.

Expenditures for general purpose equipment are allowable if they align to and support one or more core capabilities identified in the NPG, and in addition, are deployable/sharable through the Emergency Management Assistance Compact and allowable under 6 U.S.C. § 609. Refer to the NOFO for examples of allowable general-purpose equipment.

**Equipment  
Maintenance/  
Sustainment**

Use of HSGP funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable as described in FEMA [IBs 336](#) and [379](#), as well as Grant Programs Directorate (GPD) Policy [FP-205-402-125-1](#).

### **Emergency Communications Projects**

All Subrecipient emergency communications projects must comply with the SAFECOM Guidance on Emergency Communications Grants and describe in their FMFW how such activities align with the goals of the Statewide Communications Interoperability Plan.

Subrecipients are encouraged to update their Tactical Interoperable Communications Plan (TICP) and make it available upon request. Updating a TICP is an eligible activity under the FY 2020 HSGP.

### **Telecom Equipment and Services Prohibitions**

Effective August 13, 2020, the [John S. McCain National Defense Authorization Act for FY 2019 \(NDAA\)](#) prohibits DHS/FEMA Recipients and Subrecipients (including their contractors and subcontractors) from using any FEMA funds under open or new awards for the following telecommunications equipment or services:

- 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.

### **Small Unmanned Aircraft Systems**

All requests to purchase Small Unmanned Aircraft Systems (SUAS) with FEMA grant funding must comply with [IB 426](#) and include copies 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. The Authorized Equipment Listing for [03OE-07-SUAS](#) details ten questions that must be included in the Aviation Request justification. Please reference [Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems](#) for additional information.

### **Emergency Operations Plans**

Subrecipients must update their Emergency Operations Plan at least once every two years to remain compliant with the [Comprehensive Preparedness Guide 101 version 2.0](#).

### **Conflict of Interest**

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

Subrecipients must disclose to their Program Representative, in writing, any real or potential conflict of interest as defined by the federal, state, local, or tribal statutes or regulations, which may arise during the administration of the HSGP subaward within five days of learning of the conflict of interest.

### FY 2020 Investments

The State prioritized the following investment strategies for the FY 2020 subawards (the first four are National Priorities):

1. Enhance Information and Intelligence Sharing and Cooperation with Federal Agencies, including DHS (**National Priority**);
2. Enhance the Protection of Soft Targets/Crowded Places (including election security) (**National Priority**);
3. Enhance Cybersecurity (including election security) (**National Priority**);
4. Address Emergent Threats (**National Priority**);
5. Enhance Medical and Public Health Preparedness;
6. Strengthen Emergency Communications Capabilities Through Planning, Governance, Technology, and Equipment;
7. Enhance Community Resilience, Including Partnerships with Volunteers and Community-Based Organizations and Programs;
8. Strengthen Information Sharing and Collaboration (non-Fusion Center);
9. Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Planning, Response & Recovery Capabilities; and
10. Protect Critical Infrastructure and Key Resources (includes Food and Agriculture).

### California Homeland Security Strategy Goals

The State prioritized the following California Homeland Security Strategy Goals for the FY 2020 subawards:

1. Enhance Information Collection, Analysis, and Sharing, in Support of Public Safety Operations Across California;
2. Protect Critical Infrastructure and Key Resources From All Threats and Hazards;
3. Strengthen Security and Preparedness Across Cyberspace;
4. Strengthen Communications Capabilities Through Planning, Governance, Technology, and Equipment;
5. Enhance Community Preparedness;
6. Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Catastrophic Planning, Response, and Recovery Capabilities;
7. Improve Medical and Health Capabilities;
8. Enhance Incident Recovery Capabilities;
9. Strengthen Food and Agriculture Preparedness;
10. Prevent Violent Extremism Through Multi-Jurisdictional/Inter-Jurisdictional Collaboration and Coordination; and
11. Enhance Homeland Security Exercise, Evaluation, and Training Programs.

<b>State Initiative Funding</b>	For FY 2020, Cal OES shall retain 20 percent of the SHSP and approximately 17 percent of the UASI funding for state initiatives.
<b>“On Behalf Of”</b>	Cal OES may, in conjunction with local approval authorities, designate funds “on behalf of” local entities who choose to decline or fail to utilize their subaward in a timely manner.
<b>Regional Approach</b>	Subrecipients must take a regional approach and consider the needs of local units of government and applicable volunteer organizations in the projects and activities included in their FY 2020 HSGP application.
<b>Public Alert and Warning</b>	Cal OES encourages Subrecipients to consider the use of this funding to assist their jurisdiction’s alignment with the <a href="#"><u>State of California Alert and Warning Guidelines</u></a> , developed pursuant to Senate Bill 833 of the 2018 Legislative Session.

### Financial Management Forms Workbook

The FY 2020 Cal OES FMFW includes:

**Grant Subaward Face Sheet** – Use the Grant Subaward Face Sheet to apply for grant programs. The Grant Subaward Face Sheet must be signed and printed in portrait format.

**Authorized Body of 5** – Provide the contact information of Authorized Agents (AA), delegated via the GBR or Signature Authorization Form, including staff related to grant activities. More than one person is recommended for designation as the AA; in the absence of an AA, an alternate AA can sign requests.

**Project Ledger** – The project ledger is used in the application process to submit funding information and is used for submitting cash requests, grant subaward modifications, and assists with the completion of the Biannual Strategy Implementation Report (BSIR).

**Planning Ledger** – Provides detailed information on grant-funded planning activities with a final product identified.

**Organization Ledger** – Provides detailed information on grant-funded organizational activities.

**Equipment Ledger** – Detailed information must be provided under the equipment description for all grant-funded equipment. AEL numbers must be included for all items of equipment. Always refer to the AEL for a list of allowable equipment and conditions, if any.

**Training Ledger** – Provides detailed information on grant-funded training activities. All training activities must receive Cal OES approval prior to starting the event, including a Training Feedback number. The [Training Request Form](#) must be submitted and approved to obtain a Training Feedback number.

**Exercise Ledger** – Provides detailed information on grant-funded exercises.

**M&A Ledger** – Provides information on grant-funded M&A activities.

**Indirect Costs Ledger** – Provides information on indirect costs.

**Financial  
Management  
Forms Workbook  
(cont.)**

**Consultant-Contractor Ledger** – Provides detailed information on grant-funded consultants and contractors.

**Authorized Agent Page** – The AA Page must be submitted with the application, all cash requests, and Grant Subaward Modifications. The AA Page must include the appropriate signature and date.

**Subrecipient  
Grants  
Management  
Assessment**

Per [2 C.F.R. § 200.331](#), Cal OES is required to evaluate the risk of non-compliance with federal statutes, regulations, and grant terms and conditions posed by each Subrecipient of pass-through funding. The [Subrecipient Grants Management Assessment Form](#) contains questions related to an organization's experience in the management of federal grant awards. It is used to determine and provide an appropriate level of technical assistance, training, and grant oversight to Subrecipients during the subaward. The questionnaire must be completed and returned with the grant application.

**Application  
Attachments**

**Federal Funding Accountability and Transparency Act (FFATA)**  
**Financial Disclosure** – Use the [FFATA Financial Disclosure Form](#) to provide the information required by the Federal Funding Accountability and Transparency Act of 2006.

**Certification Regarding Lobbying** – Use the [Certification Regarding Lobbying Form](#) to certify lobbying activities, as stipulated by the Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352.

**Intelligence Analysts Certificates** – Pursuant to the Preparedness Grants Manual, Cal OES must have certificates for completion of training for fusion center analytical personnel. Please provide copies of certificates for each intelligence analyst, if applicable.

**UASI Footprint (UASIs Only)** – The Urban Area Working Group (UAWG) establishes the 'footprint' of the UA. A map or list defining the footprint must be included with the application.

**UAWG Member Roster (UASIs Only)** – A list of all current UAWG members with positions or titles.

**Indirect Cost Rate Agreement** – If claiming indirect costs at a federally-approved rate, please provide a copy of the approved indirect cost rate agreement.

### **Standard Assurances**

The Standard Assurances list the requirements to which the Subrecipients will be held accountable. All Applicants will be required to submit a signed, **original** of the [FY 2020 Standard Assurances](#) as part of their FY 2020 HSGP application. The required Standard Assurances can be found only in PDF format on the Cal OES website.

**NOTE:** Self-created Standard Assurances will not be accepted.

### **Operational Areas Only**

**Approval Authority Body** – OAs must appoint an Anti-Terrorism Approval Body (Approval Authority) to have final approval of the OA’s application for HSGP funds. Each member of the Approval Authority must provide written agreement with the OA’s application for HSGP funds. The Approval Authority shall consist of the following representatives, and additional voting members may be added by a simple majority vote of the following standing members:

- County Public Health Officer or designee responsible for Emergency Medical Services
- County Fire Chief or Chief of Fire Authority
- Municipal Fire Chief (selected by the OA Fire Chiefs)
- County Sheriff
- Chief of Police (selected by the OA Police Chiefs)

**Governing Body Resolution** – The GBR appoints AAs (identified by the individual’s name or by a position title) to act on behalf of the governing body and the Applicant by executing any actions necessary for each application and subaward. All Applicants are required to submit a copy of an approved GBR with their grant application. Resolutions may be valid for up to three grant years given the following:

- The resolution identifies the applicable grant program (e.g., EMPG and/or HSGP);
- The resolution identifies the applicable grant years, (e.g., FY 2020, FY 2021, FY 2022); and
- Adheres to any necessary elements required by local protocols, rules, etc., if applicable.

### **Operational Areas Only (cont.)**

Resolutions that only identify a single grant program will only be valid for that single program. Resolutions that do not identify applicable grant years will only be valid for the grant year in which the resolution was submitted.

**Authorized Agent Information** – For each person or position appointed by the governing body, identify the individual in the Authorized Body of 5 ledger of the FMFW.

All changes in AA and contact information must be provided to Cal OES in writing. If the GBR identifies the AA by name, a new Resolution is needed when changes are made. If the GBR identifies the AA by position and/or title, changes may be made by submitting a request on the entity's letterhead, signed by an existing AA. Cal OES will not accept signatures of an AA's designee, unless authorized by the Governing Body's resolution. A change to an AA's designee must be submitted on agency letterhead and signed by the AA, announcing the change to their designee.

### **Urban Areas Only**

**Urban Area Working Groups (UAWGs)** – 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 UA. It also must be inclusive of local Citizen Corps Council and tribal representatives. The UAWG should also ensure the integration of local emergency management, public health, and health care systems into a coordinated sustained local capability to respond effectively to a mass casualty incident. Additional group composition criteria is found in the FEMA [Preparedness Grants Manual](#).

**THIRA** – Subrecipients are required to submit a THIRA for all 32 core capabilities. Beginning in 2019, UAs are required to submit a THIRA every three years. An annual capability assessment will still be required.

**SPR** – The SPR is an annual grant requirement for all states, territories, and UAs. It is an annual capability assessment, which helps jurisdictions identify capability gaps and prioritize investment requirements to reach the targets set in their THIRA.

**Fusion Centers  
Only**

All projects included in the fusion center investment (IJ #1) must align to, and reference, specific performance areas of the assessment that the funding is intended to support.

Fusion Centers are also required to follow all Reporting and Administrative Metrics for California Fusion Centers, as set forth in the Governor's Homeland Security Advisor/Cal OES Director's letter dated March 16, 2016. These operational and administrative metrics set forth an integrated and coordinated approach for regular and proactive information and intelligence sharing between all fusion centers in the California State Threat Assessment System (STAS).

**State Agencies  
and Tribes Only**

State Agencies, and federally-recognized tribes may submit the Signature Authorization Form in lieu of a GBR, signed by the most senior ranking official, such as the Secretary, Director, President, Chancellor, or Chairperson.

### **Application Submission**

Subrecipients must submit an electronic copy of their completed FMFW to their Program Representative for review. After the application is approved, a completed hardcopy of the FMFW, along with all other application components must be mailed, with original signatures, by the application due date. During the application process, if it is determined not all allocated funds can be expended by the end of the period of performance, please inform a Program Representative as soon as possible. The completed application should be received by Cal OES no later than January 31, 2021. The FY 2020 HSGP Timeline is referenced as Attachment B.

### **Late or Incomplete Application**

Late or incomplete applications may be denied. If an application is incomplete, the Program Representative may request additional information. Requests for late submission of applications must be made in writing to the Program Representative prior to the application due date. Cal OES has sole discretion to accept or reject a late or incomplete grant application.

### **HSGP Contact Information**

All Subrecipient application materials, questions, comments, and correspondence should be directed to:

California Governor's Office of Emergency Services  
ATTN: Grants Management (Building E)  
Homeland Security Grants Unit  
3650 Schriever Avenue  
Mather, CA 95655

Darlene Arambula	(916) 845-8427
Christopher Camacho	(916) 845-8789
Laura Halverstadt	(916) 845-8367
Antoinette Johnson	(916) 845-8260
Jim Lane	(916) 845-8428
Miguel Ramirez	(916) 328-7466
Olivia Skierka	(916) 845-8744
Abigayle Tirapelle	(916) 845-8400

The [Program Representative Regional Assignments Map](#) is available at the Cal OES website under “Regional Assignments”.

### **Subaward Approval**

Subrecipients will receive a formal notification of award no later than 45 days after Cal OES receives the federal grant award. The award letter must be signed, dated, and returned to Cal OES within 20 calendar days. Once the completed application, along with the signed award letter, is received and approved, reimbursement of eligible subaward expenditures may be requested using the Cal OES FMFW.

**Payment Request Process**

To request an advance or cash reimbursement of FY 2020 HSGP funds, Subrecipients must first complete a payment request using the Cal OES FMFW, returning it to the appropriate Program Representative. Subrecipients who fail to follow the workbook instructions may experience delays in processing the payment request.

Payments can only be made if the Subrecipient has submitted a completed and approved application.

**Advances and Interest Earned on Advances**

An Advance payment is a payment that is requested before Subrecipients have disbursed the funds for program purposes. Subrecipients may be paid an advance, provided they maintain a willingness and ability to maintain procedures to minimize the time elapsing between the receipt of funds and their disbursement. The timing and amount of advance payments must be as close as administratively feasible to the actual disbursements by the Subrecipient for project costs.

Federal rules require advances to be deposited in interest-bearing accounts. Interest earned amounts up to \$500 per year may be retained by Subrecipients for administrative expenses; any additional interest earned on federal advance payments must be returned annually to Cal OES.

**Semi-Annual Drawdown Requirements**

All Subrecipients should be reporting expenditures and requesting funds at least semi-annually throughout the period of performance. Semi-annual drawdowns should be occurring by March and October of each calendar year following final approval of the subaward application, except for the final cash request, which must be submitted within 20 calendar days after the end of the period of performance. Subrecipients not in compliance with this requirement will be required to submit all supporting documentation for subsequent cash requests.

**Modifications**

Post-award budget, scope, and time modifications must be requested using the [Cal OES HSGP FMFW v1.20](#), signed by the Subrecipient's AA, and submitted to the Program Representative.

The Subrecipient may implement grant modification activities, and incur associated expenses, only after receiving written final approval of the modification from Cal OES.

**Modifications  
(cont.)**

Subrecipients must provide a written justification with all modification requests. The justification may be included in the body of the e-mail transmitting the request, or in a document attached to the transmittal e-mail. Please reference [GMM 2018-17](#) for additional information regarding modification requests.

**A modification request for any project within the national priority areas must receive DHS/FEMA prior approval. These requests include, but are not limited to, a change in project scope, any change to the project budget, and re-programming of funds. DHS/FEMA and Cal OES may request additional information to validate project effectiveness.**

**Training**

All grant-funded training activities must receive Cal OES approval prior to starting the training event. Cal OES shall allow Subrecipients to develop a “placeholder” for future training conferences when an agenda has not been established at the time Subrecipient applications are due. Please work with a Program Representative and the Training Branch to identify a possible “placeholder” for these types of training activities.

When seeking approval of non-DHS/FEMA developed courses, course materials must be submitted with the approval requests. Conditional approvals are not offered.

Subrecipients must complete a [Training Request Form](#) and submit it electronically to the Cal OES Training Branch to be approved with a Training Feedback Number before beginning any training activities. This includes project components like travel to, materials for, or attendance in training courses. Training Feedback Numbers must be obtained no later than 30 days before the first day of the training or related activities. Training Feedback numbers must be included on the FMFW Training Ledger in order to be considered for reimbursement.

For more information on this or other training-related inquiries, contact the [Cal OES Training Branch](#) at (916) 845-8752.

**Exercises,  
Improvement  
Plans, and After  
Action Reporting**

Subrecipients should engage stakeholders to identify long-term training and exercise priorities. These priorities should address capability targets and gaps identified through the THIRA and SPR process, real-world events, previous exercises, and national areas for improvement identified in the NPR.

**Exercises,  
Improvement  
Plans, and After  
Action Reporting  
(cont.)**

Subrecipients must report on all exercises conducted with HSGP grant funds. An After Action Report (AAR)/Improvement Plan (IP) or Summary Report (for Seminars and Workshops) must be completed and submitted to Cal OES within 90 days after exercise/seminars/workshops are conducted. It is acceptable to submit an *Exercise Summary Report for Seminars and Workshops* in lieu of a full AAR/IP.

Please e-mail AAR/IPs and Summary Reports to:

- [hseep@fema.dhs.gov](mailto:hseep@fema.dhs.gov)
- [exercise@caloes.ca.gov](mailto:exercise@caloes.ca.gov)
- [christopher.camacho@caloes.ca.gov](mailto:christopher.camacho@caloes.ca.gov)

For exercise-related issues and/or questions, please email the Cal OES Exercise Team at [exercise@caloes.ca.gov](mailto:exercise@caloes.ca.gov).

Exercise costs will not be reimbursed until an AAR/IP has been submitted.

**Procurement  
Standards and  
Written  
Procedures**

Subrecipients must conduct procurement utilizing documented local government procurement standards and procedures, or the federal procurement standards found in [2 C.F.R. Part 200](#), whichever is more strict. Procurement standards must also contain a written conflict of interest policy which reflect applicable federal, state, local, and tribal laws.

**Procurement  
Thresholds**

Effective June 20, 2018, the micro-purchase threshold was increased from \$3,500 to \$10,000 and the simplified acquisition threshold was increased from \$150,000 to \$250,000. These increases apply to all Subrecipient procurements executed on or after June 20, 2018. Refer to [IB 434](#) for additional information.

**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. 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:

**Procurement Documentation (cont.)**

- 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 Subrecipient.

**Noncompetitive Procurement**

All noncompetitive procurements exceeding the simplified acquisition threshold requires Cal OES **prior** written approval to be eligible for reimbursement. This method of procurement must be approved by the local Purchasing Agent prior to submitting a request for Cal OES approval. A copy of the Purchasing Agent's approval must be included with the Cal OES [Request for Noncompetitive Procurement Authorization](#) form. Cal OES may request additional documentation that supports the procurement effort.

**Note:** Cal OES will not reimburse for any noncompetitive procurement contracts for any terrorism-related training, regardless of the cost of the training. Exceptions to this policy may be approved in limited circumstances, e.g., related to a procurement effort that has resulted in inadequate competition.

**Performance Bond**

Due to the risks associated with delays in vendor delivery of large equipment procurements, DHS/FEMA allows Subrecipients to obtain a “performance bond” for items that are paid for up front to ensure delivery of the equipment within the grant performance period.

Cal OES requires Subrecipients obtain a performance bond for any equipment item over \$250,000 or any vehicle, aircraft, or watercraft financed with HSGP funds. Subrecipients must provide a copy of all performance bonds to their Program Representative no later than the time of reimbursement.

Performance Bond Waivers may be granted on a case-by-case basis and must be submitted to Cal OES prior to procurement.

**Environmental Planning and Historic Preservation**

DHS/FEMA is required to ensure all activities and programs that are funded by the agency comply with federal Environmental Planning and Historic Preservation (EHP) regulations. Subrecipients proposing projects or activities (including, but not limited to, training, exercises, the installation of equipment, and construction or renovation projects) that have the potential to impact the environment or a historic structure must participate in the EHP screening process. EHP Screening Memos must include detailed project information, explain the goals and objectives of the proposed project, and include supporting documentation.

DHS/FEMA may also require the Subrecipient to provide a confidential California Historical Resources Information System (CHRIS) report in addition to the EHP Screening Form.

Determination on the necessity of a CHRIS report is based upon information disclosed on the form. Program Representatives will provide additional instructions should this report be required.

[EHP Screening Requests](#) should be submitted to Cal OES as early as possible. All projects/activities triggering EHP must receive DHS/FEMA written approval prior to commencement of the funded activity.

Updated information may be referenced in the [FEMA GPD EHP Policy Guidance](#).

**Construction and Renovation**

When applying for construction activity at the time of application, including communication towers, Subrecipients must submit evidence of approved zoning ordinances, architectural plans, any other locally required planning permits, and a notice of federal interest. Additionally, Subrecipients are required to submit an SF-424C Budget and Budget Detail that cites project costs. Communication tower construction requests also require evidence that the Federal Communications Commission's Section 106 review process was completed.

Subrecipients using funds for construction projects must comply with the Davis-Bacon Act. Subrecipients 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.

**Construction and Renovation (cont.)**

Project construction using SHSP and UASI funds may not exceed \$1,000,000 or 15 percent of the grant subaward (For the purposes of limitations on funding levels, communications towers are not considered construction).

***Written approval for construction must be provided by DHS/FEMA prior to the use of any HSGP funds for construction or renovation.***

**Inventory Control and Property Management**

FY 2020 HSGP Subrecipients must use standardized resource management concepts for resource typing and credentialing, in addition to maintaining an inventory by which to facilitate the effective identification, dispatch, deployment, tracking, and recovery of resources.

Subrecipients must have an effective inventory management system, to include:

- Property records that document description, serial/ID number, fund source, title information, acquisition date, cost, federal cost share, location, use, condition, and ultimate disposition;
- Conducting a physical inventory at least every two years;
- A control system to prevent loss, damage, and theft of grant purchased equipment and supplies; and
- Adequate maintenance procedures must be developed to keep the property in good condition.

**Equipment Disposition**

When original or replacement equipment acquired under the HSGP is no longer needed for program activities, the Subrecipient must contact the Program Representative to request disposition instructions. See [2 C.F.R. § 200.313\(e\)](#).

**Performance Reporting**

Subrecipients must complete a BSIR each Winter and Summer using the DHS/FEMA [Grants Reporting Tool](#) (GRT) for the duration of the subaward period of performance or until all grant activities are completed and the subaward is formally closed by Cal OES. Failure to submit a BSIR could result in subaward reduction, suspension, or termination.

**Performance Reporting (cont.)**

Access to the BSIR may be obtained through the GRT. To create a new account, please click the link that reads, “Register for an account” and follow the instructions provided. The Subrecipient will be required to ensure up-to-date project information is entered. The Project Ledger in the FMFW may assist with the BSIR data entry process. For additional assistance with the GRT, please contact your Program Representative.

**Extension Requests**

Extensions to the initial period of performance identified in the subaward will only be considered through formal, written requests to your Program Representative. Upon receipt of the extension request, Cal OES will:

1. Verify compliance with performance reporting requirements by confirming the Subrecipient has submitted all necessary performance reports;
2. Confirm the Subrecipient has provided sufficient justification for the request; and
3. If applicable, confirm the Subrecipient has demonstrated sufficient progress in past situations where an extension was authorized by Cal OES.

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

1. Contractual commitments with vendors that prevent completion of the project within the period of performance;
2. The project must undergo a complex environmental review which cannot be completed within this timeframe;
3. Projects are long-term by design and therefore, acceleration would compromise core programmatic goals; and
4. Where other special circumstances exist.

To be considered, extension requests must be received no later than 60 days prior to the end of the Subrecipient's period of performance and must contain specific and compelling justifications as to why an extension is required. All extension requests must address the following:

**Extension Requests (cont.)**

1. Grant program, fiscal year, and award number;
2. Reason for delay;
3. Current status of the activity/activities;
4. Approved period of performance 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 each milestone and the position/person responsible for implementing the plan for completion; and
9. Certification the activity/activities will be completed within the extended period of performance without any modification to the original Statement of Work.

General questions regarding extension requirements and the extension request form, should be directed to your Program Representative. For additional information, please see IB 379. Extension requests for personnel and salaries do not meet the requirements of IB 379 and will not be granted. Subrecipients are expected to complete all grant-funded personnel activity by the end of the subaward period of performance.

**Progress Reports on Grant Extensions**

All Subrecipients that receive Cal OES approval to extend their FY 2020 grant subaward period of performance may be required to submit progress reports indicating completed and future project milestones on all extended projects. Progress reports must be submitted electronically to the Subrecipient's Program Representative. Deadlines for the submission of progress reports will be established at the time of extension approval.

**Monitoring**

Cal OES Grants Monitoring actively monitors Subrecipients, through day-to-day communications, programmatic site visits, and desk and on-site compliance assessments. The purpose of the compliance assessment is to ensure Subrecipients are in compliance with applicable state and federal regulations, grant guidelines, and programmatic requirements. Monitoring activities may include, but are not limited to:

- Verifying that entries recorded on the FMFW categories are properly supported with source documentation;
- Eligibility of and support for expenditures, typically covering two to three years of data;

**Monitoring  
(cont.)**

- Comparing actual Subrecipient activities to those approved in the grant application and subsequent modifications, including the review of timesheets and invoices as applicable;
- Procurements and contracts;
- Ensuring equipment lists are properly maintained and physical inventories are conducted;
- Ensuring advances have been disbursed in accordance with applicable guidelines; and
- Confirming compliance with:
  - Standard Assurances, and
  - Information provided on performance reports and payment requests

NOTE: It is the responsibility of all Subrecipients that pass down grant funds to other entities, to maintain and utilize a formal process to monitor the grant activities of their subawards. This requirement includes, but is not limited to, on-site verification of grant activities, as required. It is common for Subrecipients to receive findings in a programmatic site visit or compliance assessment, which require a Corrective Action Plan (CAP) to be submitted by Subrecipients. Those Subrecipients who fail to submit a CAP, as required, shall have a “hold” placed on any future reimbursements until the “finding” is resolved.

**Failure to Submit  
Required Reports**

Periodic reporting is required by the grant. Subrecipients who miss a single reporting deadline may receive a letter addressed to their Board of Supervisors informing them of the failure to report. County OAs and tribes who fail to report twice in a row may have subsequent awards reduced by 10 percent until timely reporting is reestablished; UASIs may have a “hold” placed on any future reimbursements.

**Suspension/  
Termination**

Cal OES may suspend or terminate grant funding, in whole or in part, or other measures may be imposed for any of the following reasons:

- Failure to submit required reports.
- Failure to expend funds in a timely manner consistent with the grant milestones, guidance, and assurances.
- Failure to comply with the requirements or statutory progress toward the goals or objectives of federal or state law.
- Failure to make satisfactory progress toward the goals or objectives set forth in the Subrecipient application.

**Suspension/  
Termination  
(cont.)**

- Failure to follow Grant Subaward requirements or Special Conditions.
- Proposing or implementing substantial plan changes to the extent that, if originally submitted, the application would not have been selected for funding.
- False certification in the application or document.
- Failure to adequately manage, monitor, or direct the grant funding activities of their Subrecipients.

Before taking action, Cal OES will provide the Subrecipient reasonable notice of intent to impose corrective measures and will make every effort to informally resolve the problem.

**Closeout**

Cal OES will close-out Subrecipient awards when it determines all applicable administrative actions and all required work of the federal award have been completed.

Subawards will be closed after:

- All funds have been requested and reimbursed, or disencumbered;
- Receiving all applicable Subrecipient reports indicating all approved work has been completed, and all funds have been distributed;
- Completing a review to confirm the accuracy of reported information;
- Reconciling actual costs to subawards, modifications, and payments; and
- Verifying the Subrecipient has submitted a final BSIR showing all grant funds have been expended.

**Records  
Retention**

The records retention period is three years from the date of the Cal OES Grant Closeout letter, or until any pending litigation, claim, or audit started before the expiration of the three-year retention period has been resolved and final action is taken.

For indirect cost rate proposals, cost allocation plans, or other rate computation records, the start of the record retention period is dependent on whether the proposal, plan, or other computation is required to be submitted to the federal government (or to the pass-through entity) for negotiation purposes. See [2 C.F.R. § 200.334\(f\)](#).

### **Records Retention (cont.)**

In order for any cost to be allowable, it must be adequately documented per [2 C.F.R. § 200.403\(g\)](#).

The Cal OES Grant Closeout Letter will notify the Subrecipient of the start of the records retention period for all programmatic and financial grant-related records.

If the State Administrative Agency's award remains open after the Subrecipient's submission of the final BSIR, Cal OES will complete any additional BSIR reporting required under the award on behalf of the Subrecipient.

Closed grants may still be monitored and audited. Failure to maintain all grant records for the required retention period could result in a reduction of grant funds, and an invoice to return costs associated with the unsupported activities.

If documents are retained longer than the required retention period, FEMA, the DHS Office of Inspector General, Government Accountability Office, and pass-through entity have the right to access these records as well. See [2 C.F.R. §§ 200.333, 200.336](#).

State Homeland Security Program (SHSP)					
Operational Area	Population	Base Amount	25% LE	SHSP	Total Award (25% LE + SHSP)
ALAMEDA	1,669,301	75,000	446,857	1,340,569	1,787,426
ALPINE	1,162	75,000	19,048	57,144	76,192
AMADOR	38,294	75,000	28,571	85,712	114,283
BUTTE	226,466	75,000	76,829	230,488	307,317
CALAVERAS	45,117	75,000	30,321	90,961	121,282
COLUSA	22,117	75,000	24,422	73,267	97,689
CONTRA COSTA	1,155,879	75,000	315,185	945,555	1,260,740
DEL NORTE	27,401	75,000	25,777	77,332	103,109
EL DORADO	191,848	75,000	67,951	203,853	271,804
FRESNO	1,018,241	75,000	279,887	839,659	1,119,546
GLENN	29,132	75,000	26,221	78,664	104,885
HUMBOLDT	135,333	75,000	53,457	160,372	213,829
IMPERIAL	190,266	75,000	67,545	202,636	270,181
INYO	18,593	75,000	23,519	70,555	94,074
KERN	916,464	75,000	253,785	761,355	1,015,140
KINGS	153,710	75,000	58,170	174,510	232,680
LAKE	65,071	75,000	35,438	106,315	141,753
LASSEN	30,150	75,000	26,482	79,446	105,928
LOS ANGELES	10,253,716	75,000	2,648,403	7,945,209	10,593,612
MADERA	159,536	75,000	59,664	178,993	238,657
MARIN	262,879	75,000	86,168	258,502	344,670
MARIPOSA	18,068	75,000	23,384	70,151	93,535
MENDOCINO	89,009	75,000	41,577	124,732	166,309
MERCED	282,928	75,000	91,309	273,928	365,237
MODOC	9,602	75,000	21,213	63,637	84,850
MONO	13,616	75,000	22,242	66,726	88,968
MONTEREY	445,414	75,000	132,980	398,940	531,920
NAPA	140,779	75,000	54,854	164,562	219,416
NEVADA	98,904	75,000	44,115	132,344	176,459
ORANGE	3,222,498	75,000	845,187	2,535,562	3,380,749
PLACER	396,691	75,000	120,485	361,454	481,939
PLUMAS	19,779	75,000	23,823	71,467	95,290
RIVERSIDE	2,440,124	75,000	644,541	1,933,621	2,578,162
SACRAMENTO	1,546,174	75,000	415,280	1,245,838	1,661,118
SAN BENITO	62,296	75,000	34,726	104,179	138,905
SAN BERNARDINO	2,192,203	75,000	580,959	1,742,878	2,323,837
SAN DIEGO	3,351,786	75,000	878,344	2,635,032	3,513,376
SAN FRANCISCO	883,869	75,000	245,426	736,277	981,703
SAN JOAQUIN	770,385	75,000	216,322	648,965	865,287

Attachment A – FY 2020 HSGP Allocations | **2020**

Operational Area	Population	Base Amount	25% LE	SHSP	Total Award (25% LE + SHSP)
<b>SAN LUIS OBISPO</b>	280,393	75,000	90,659	271,978	<b>362,637</b>
<b>SAN MATEO</b>	774,485	75,000	217,373	652,120	<b>869,493</b>
<b>SANTA BARBARA</b>	454,593	75,000	135,334	406,003	<b>541,337</b>
<b>SANTA CLARA</b>	1,954,286	75,000	519,943	1,559,830	<b>2,079,773</b>
<b>SANTA CRUZ</b>	274,871	75,000	89,243	267,729	<b>356,972</b>
<b>SHASTA</b>	178,773	75,000	64,598	193,794	<b>258,392</b>
<b>SIERRA</b>	3,213	75,000	19,574	58,722	<b>78,296</b>
<b>SISKIYOU</b>	44,584	75,000	30,184	90,552	<b>120,736</b>
<b>SOLANO</b>	441,307	75,000	131,927	395,780	<b>527,707</b>
<b>SONOMA</b>	500,675	75,000	147,153	441,457	<b>588,610</b>
<b>STANISLAUS</b>	558,972	75,000	162,103	486,309	<b>648,412</b>
<b>SUTTER</b>	97,490	75,000	43,752	131,257	<b>175,009</b>
<b>TEHAMA</b>	64,387	75,000	35,263	105,787	<b>141,050</b>
<b>TRINITY</b>	13,688	75,000	22,261	66,781	<b>89,042</b>
<b>TULARE</b>	479,112	75,000	141,622	424,867	<b>566,489</b>
<b>TUOLUMNE</b>	54,590	75,000	32,750	98,251	<b>131,001</b>
<b>VENTURA</b>	856,598	75,000	238,432	715,295	<b>953,727</b>
<b>YOLO</b>	222,581	75,000	75,833	227,498	<b>303,331</b>
<b>YUBA</b>	77,916	75,000	38,732	116,197	<b>154,929</b>
<b>Total</b>	<b>39,927,315</b>	<b>4,350,000</b>	<b>11,327,203</b>	<b>33,981,597</b>	<b>45,308,800</b>

Fusion Centers		
Region	Total Award	
<b>SAN FRANCISCO BAY AREA</b>	1,792,050	
<b>SACRAMENTO/CENTRAL VALLEY AREA</b>	2,565,000	
<b>GREATER LOS ANGELES AREA</b>	2,887,500	
<b>SAN DIEGO AREA</b>	2,047,500	
<b>ORANGE AREA</b>	715,000	
<b>Total</b>	<b>10,007,050</b>	

<b>Urban Areas Security Initiative (UASI)</b>			
<b>*A minimum of 25% of UASI funding must be for Law Enforcement Terrorism Prevention</b>			
<b>Urban Area</b>	<b>Federal Allocation to State</b>	<b>Allocation to UASI</b>	<b>State Initiatives</b>
<b>ANAHEIM/SANTA ANA AREA</b>	5,250,000	4,341,750	908,250
<b>BAY AREA</b>	37,500,000	31,012,500	6,487,500
<b>LOS ANGELES/LONG BEACH AREA</b>	68,000,000	56,236,000	11,764,000
<b>RIVERSIDE AREA</b>	3,500,000	2,894,500	605,500
<b>SACRAMENTO AREA</b>	3,500,000	2,894,500	605,500
<b>SAN DIEGO AREA</b>	16,900,000	13,976,300	2,923,700
<b>Total</b>	<b>134,650,000</b>	<b>111,355,550</b>	<b>23,294,450</b>

## Attachment B: FY 2020 HSGP Timeline | **2020**

---

DHS/FEMA Announcement of 2020 HSGP	February 14, 2020
Cal OES Application Due to DHS	April 30, 2020
DHS Award to California	September 8, 2020
Subrecipient period of performance begins	September 1, 2020
2020 HSGP California Supplement release	December 2020
Subrecipient Workshops	November 2020
Subrecipient Awards (45 days from DHS award)	October 23, 2020
Subrecipient Final Applications Due to Cal OES	January 31, 2021
Subrecipient period of performance ends	May 31, 2023
Final Cash Requests due to Cal OES	Within twenty (20) calendar days after end of grant
Cal OES's period of performance ends	August 31, 2023

**Subrecipient:** \_\_\_\_\_ **FIPS#:** \_\_\_\_\_

**Program Representative:** \_\_\_\_\_

**Financial Management Forms Workbook:**

- Grant Award Face Sheet
- Authorized Body of 5
- Project Ledger
- Planning Ledger
- Organization Ledger
- Equipment Ledger
- Training Ledger
- Exercise Ledger
- Consultant/Contractor Ledger
- Management & Administration Ledger
- Indirect Cost Ledger
- Authorized Agent Sheet

**Attachments:**

- Original Counter-Signed Award Letter
- Governing Body Resolution (Certified)
- Standard Assurances (Signed Originals)
- FFATA Certification
- Lobbying Certification
- Subrecipient Grant Management Assessment Form
- Indirect Cost Rate Negotiation Agreement
- Personnel Cap Waiver (If Applicable)
- National Priority Waiver (If Applicable)
- Intelligence Analyst(s) Certificates (If Applicable)

**UASI Only:**

- UASI Footprint
- UAWG Roster

**State Agencies and Tribes Only:**

- Signature Authority Form (in lieu of Governing Body Resolution)

**For Cal OES Use Only**

Reviewed by: \_\_\_\_\_ Date: \_\_\_\_\_

Management Approval: \_\_\_\_\_ Date: \_\_\_\_\_

GAVIN NEWSOM  
GOVERNOR

MARK S. GHILARDUCCI  
DIRECTOR



October 23, 2020

Andrew Lockman  
Emergency Services Manager  
Tulare County  
5957 S Mooney Boulevard  
Visalia, CA 93277

**SUBJECT: NOTIFICATION OF SUBRECIPIENT SUBAWARD APPROVAL**

Fiscal Year (FY) 2020 Homeland Security Grant Program (HSGP)  
Subaward #2020-0095, Cal OES ID#107-00000  
Subaward Period of Performance: 09/01/2020-05/31/2023

Dear Mr. Lockman:

We are pleased to announce the approval of your FY 2020 HSGP subaward in the amount of \$566,489. Once the completed application is received and approved, reimbursement of eligible subaward expenditures may be requested using the California Governor's Office of Emergency Services (Cal OES) Financial Management Forms Workbook. Failure to provide documentation in a timely manner could result in a hold on funding, pursuant to Title 2, Code of Federal Regulations (CFR), Sections 200.338(a) and 200.207(b)(1)-(2).

This subaward is subject to requirements in 2 CFR, Part 200, including the Notice of Funding Opportunity (NOFO), the Preparedness Grants Manual, the California Supplement to the NOFO, and all applicable federal, state, and local requirements. All activities funded with this subaward must be completed within the subaward period of performance.

Subrecipients must obtain additional written approval **prior** to incurring costs for activities such as aviation, watercraft, allowability request logs, noncompetitive procurement, and projects requiring Environmental Planning and Historic Preservation review. Additionally, all projects falling under the National Priority Investment Justifications must be reviewed and approved for effectiveness by the



3650 SCHRIEVER AVENUE, MATHER, CA 95655  
[www.CalOES.ca.gov](http://www.CalOES.ca.gov)

Andrew Lockman  
October 23, 2020  
Page 2 of 2

Federal Emergency Management Agency (FEMA), prior to the obligation, and expenditure of funds for those projects.

Your organization will be required to prepare and submit the Biannual Strategy Implementation Report (BSIR) to Cal OES via the FEMA Grants Reporting Tool (GRT) semi-annually for the duration of the subaward period of performance or until all activities are completed and the subaward is formally closed. Failure to submit required reports could result in subaward reduction, suspension, or termination. Throughout the subaward cycle, milestones set in the GRT will be used as indicators of project feasibility, performance, and grant management capacity. This information may also be used in assessing proposals in future grant opportunities.

A Conditional Hold has been placed on your subaward; five percent of the subaward must be allocated to each of the four National Priority Investment Justifications for a total of twenty percent of the award. To release this hold, additional information is required for the investments identified which must be submitted in the December 2020 BSIR in a manner consistent with Grants Program Directorate Information Bulletin No. 447.

Your dated signature is required on this letter. Please sign and return the original to your Cal OES Program Representative within 20 calendar days upon receipt and keep a copy for your records. For further assistance, please contact your Cal OES Program Representative.

Sincerely,



MARK S. GHILARDUCCI  
Director



Andrew Lockman  
Tulare County

10/26/20

Date

## 2020 APPROVAL AUTHORITY MEMBERS HOMELAND SECURITY GRANT PROGRAM

APPROVAL AUTHORITY MEMBERS	Member/Alternate	Name	Title	Address	Phone	E-mail
Police Chief	Member-	Mike Marquez	Police Chief, City of Woodlake	350 N. Valencia Blvd., Woodlake, CA 93286	(559) 564-3346	<a href="mailto:mmarquez@ci.woodlake.ca.us">mmarquez@ci.woodlake.ca.us</a>
	Alternate-					
Municipal Fire Chief	Member-	David LaPere	Fire Chief, City of Porterville	40 W. Cleveland Ave. Porterville, CA 93257	(559) 782-7526	<a href="mailto:dlapere@ci.porterville.ca.us">dlapere@ci.porterville.ca.us</a>
	Alternate-					
County Sheriff	Member-	Mike Boudreaux	Sheriff	833 S. Akers St. Visalia, CA 93277	(559) 802-9400	<a href="mailto:mboudreaux@co.tulare.ca.us">mboudreaux@co.tulare.ca.us</a>
	Alternate-	Tom Sigley	Undersheriff	833 S. Akers St. Visalia, CA 93277	(559) 636-9400	<a href="mailto:tsigley@tularecounty.ca.gov">tsigley@tularecounty.ca.gov</a>
County Fire Chief	Member-	Charles Norman	Fire Chief	907 W. Visalia Rd. Farmersville, CA 93223	(559) 802-9801	<a href="mailto:cnormalize@co.tulare.ca.us">cnormalize@co.tulare.ca.us</a>
	Alternate-	Pete Marquez	Division Chief	907 W. Visalia Rd. Farmersville, CA 93223	(559) 802-9803	<a href="mailto:pmarquez@co.tulare.ca.us">pmarquez@co.tulare.ca.us</a>
County Public Health Officer	Member-	Dr. Karen Haught	Health Officer	5957 S. Mooney Blvd. Visalia, CA 93277	(559) 624-8481	<a href="mailto:khaught@tularehhsa.org">khaught@tularehhsa.org</a>
	Alternate-	Dan Lynch	Director, CCEMSA	1221 Fulton Mall, 5th Floor P.O. Box 11867 Fresno, CA 93775	(559) 600-3387	<a href="mailto:dlynch@co.fresno.ca.us">dlynch@co.fresno.ca.us</a>



## SYSTEM FOR AWARD MANAGEMENT (SAM) REQUIREMENTS

If your agency is using HSGP grant funds to contract with anyone, you MUST verify that they are **NOT** debarred on the Government's "**System for Award Management**" by checking the website:

<http://www.sam.gov>

- Checks must be performed at the time of the Project Proposal, if there is a vendor change, and before payment.
- Locate the "SEARCH RECORDS" menu item. You may search by an entity's name, DUNS number, or CAGE code.
- Enter the requested information (i.e. individual, firm, or entity's name; DUNS Number or CAGE Code). Click on search. The search will display the results.
- If your search returned no results, click on "Printer-Friendly" and print the search results. If the search leads you to any Active Exclusion Records for that person or entity, this means they may be debarred or suspended and may **NOT** be eligible to receive any grant funds.
- Attach the search results to your reimbursement request. The printed search results are very important because the date will be printed on the report and it must be prior to the date you contract with anyone. This report must accompany your reimbursement request to be eligible for reimbursement.
- If the contractor is listed on the website as debarred or suspended and you use their services, you will **NOT** be eligible for reimbursement from Tulare County OES.
- Contractors are only allowed a maximum reimbursement of **eight (8)** hours per day.





## Financial Management Guide

U.S. Department of Homeland Security

Preparedness Directorate

Office of Grants and Training

Office of Grant Operations

January 2006



## Department of Homeland Security

The mission of the Department of Homeland Security (DHS) is to lead the unified national effort to secure America; to prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation; and to ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce. DHS is also dedicated to protecting the rights of American citizens and enhancing public services, such as natural disaster assistance and citizenship services, by dedicating offices to these important missions.

Department of Homeland Security  
World Wide Web page:  
<http://www.DHS.gov>

**U.S. Department of Homeland Security  
Preparedness Directorate  
Office of Grants and Training  
Office of Grant Operations**

800 K Street, NW  
Washington, DC 20001

Mailing Address  
810 Seventh Street, NW  
Washington, DC 20531

**Michael Chertoff**  
Secretary  
U.S. Department of Homeland Security

**Tracy A. Henke**  
Executive Director  
Office of Grants and Training

**Kimberly Orben**  
Director, Office for Business Administration  
Office of Grants and Training

**Nancy Anne (Baugher) Foy**  
Director, Office of Grant Operations  
Office of Grants and Training  
1-866- 9ASK-OGO (866-927-5646)  
[ASK-OGO@DHS.GOV](mailto:ASK-OGO@DHS.GOV)

## **Foreword**

Since terrorists attacked our nation on September 11, 2001, the Office of Grants and Training (G&T) and its predecessor agencies have awarded more than \$8.6 billion in grant funding to build capabilities at the state and local levels to prevent, prepare for, and respond to terrorist incidents and catastrophic disasters. As stewards of these public funds, G&T and its recipient agencies share responsibility for ensuring—through sound planning and prioritizing—that those funds are well-invested, and—through sound financial processes—that those funds are well-managed.

G&T's Office of Grant Operations (OGO) developed this *Financial Management Guide* to provide step-by-step guidance in fulfilling your fiduciary responsibility as recipients of Federal grant funds and in ensuring that these taxpayer dollars are used for the purposes for which they are awarded. The *Guide* should serve as the primary reference and day-to-day management tool for G&T award recipients and subrecipients in all financial management and grant administration matters.

I hope that you will find this *Financial Management Guide* useful and welcome your comments and suggestions. I also encourage you to contact our Office of Grant Operations whenever you have a question about your financial management operations or any of the areas covered in this *Guide*. OGO's Customer Service staff may be reached at 1-866-9ASK-OGO or via e-mail at [ASK-OGO@DHS.GOV](mailto:ASK-OGO@DHS.GOV).

Thank you for your efforts to strengthen the financial management of your grants, to safeguard public funds, and to ensure our national security by building state and local preparedness. I look forward to continuing to work with you.

Tracy A. Henke  
Executive Director

## Table of Contents

<b>CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
<b>WHAT IS THE PURPOSE OF THIS GUIDE? .....</b>	<b>2</b>
<b>WHO IS THIS GUIDE DESIGNED FOR? .....</b>	<b>3</b>
<b>CHAPTER 2: THE APPLICATION PROCESS .....</b>	<b>5</b>
<b>NOTICE OF FUNDING AVAILABILITY/ANNOUNCEMENTS .....</b>	<b>6</b>
<b>APPLICATION REVIEW.....</b>	<b>6</b>
<b>TECHNICAL REVIEW.....</b>	<b>7</b>
<b>COST ANALYSIS .....</b>	<b>8</b>
<b>CHAPTER 3: THE AWARD PROCESS.....</b>	<b>9</b>
<b>THE AWARD DOCUMENT.....</b>	<b>10</b>
<b>ACCEPTANCE OF AWARD AND CONDITIONS .....</b>	<b>10</b>
<b>TYPES OF FINANCIAL ASSISTANCE: GRANT OR COOPERATIVE AGREEMENT.....</b>	<b>11</b>
<b>PLANNING AND IMPLEMENTING AWARD PROGRAMS.....</b>	<b>11</b>
<b>CHAPTER 4: MANAGING FEDERAL FUNDS .....</b>	<b>12</b>
<b>FINANCIAL MANAGEMENT SYSTEM REQUIREMENTS .....</b>	<b>13</b>
<b>RECIPIENT AND SUBRECIPIENT ACCOUNTING RESPONSIBILITIES .....</b>	<b>13</b>
<b>COMMINGLING OF FUNDS.....</b>	<b>14</b>
<b>MONITORING PROJECT PERFORMANCE .....</b>	<b>14</b>
<b>CONFLICTS OF INTEREST .....</b>	<b>15</b>
<b>SUPPLANTING .....</b>	<b>15</b>
<b>CHAPTER 5: PAYMENTS.....</b>	<b>17</b>
<b>REQUEST FOR ADVANCE/REIMBURSEMENT .....</b>	<b>18</b>
<b>WITHHOLDING OF FUNDS .....</b>	<b>18</b>
<b>CASH MANAGEMENT IMPROVEMENT ACT OF 1990.....</b>	<b>18</b>
<b>INTEREST .....</b>	<b>19</b>
<b>CHAPTER 6: OBLIGATION AND EXPENDITURES.....</b>	<b>20</b>
<b>OBLIGATION OF FUNDS .....</b>	<b>21</b>
<b>PERIOD OF AVAILABILITY.....</b>	<b>21</b>
<b>EXPENDITURE OF FUNDS .....</b>	<b>21</b>
<b>SUSPENSION AND TERMINATION.....</b>	<b>21</b>
<b>CHAPTER 7: GRANT REPORTING .....</b>	<b>23</b>
<b>FINANCIAL REPORTING .....</b>	<b>24</b>
<b>PROGRAMMATIC REPORTING .....</b>	<b>24</b>
<b>CHAPTER 8: ADJUSTMENTS TO AWARDS .....</b>	<b>25</b>
<b>MODIFICATIONS AND REVISIONS (INCLUDING GRANT ADJUSTMENT NOTICES) .....</b>	<b>26</b>
<b>NOTIFICATION OF CHANGES.....</b>	<b>26</b>
<b>TYPES OF ADJUSTMENTS: .....</b>	<b>26</b>
<b>CHAPTER 9: OTHER PROGRAM FUNDS.....</b>	<b>28</b>
<b>PROGRAM INCOME .....</b>	<b>29</b>
<b>REQUIREMENTS FOR MATCHING OR COST SHARING.....</b>	<b>30</b>
<b>CHAPTER 10: COSTS AND EXPENDITURES.....</b>	<b>32</b>
<b>ALLOWABLE COSTS .....</b>	<b>33</b>

UNALLOWABLE COSTS .....	36
COSTS REQUIRING PRIOR APPROVAL .....	38
<b>CHAPTER 11: PROCUREMENT .....</b>	<b>40</b>
PROCUREMENT STANDARDS .....	41
SOLE SOURCE PROCUREMENT (NON-COMPETITIVE) .....	41
<b>CHAPTER 12: AUDITS .....</b>	<b>43</b>
AUDIT REQUIREMENTS FOR STATES, LOCAL GOVERNMENTS, AND NON-PROFIT ORGANIZATIONS...	44
AUDITS OF COMMERCIAL/FOR-PROFIT ORGANIZATIONS.....	45
AUDITS OF SUBRECIPIENTS.....	45
DISTRIBUTION OF REPORTS .....	45
TECHNICAL ASSISTANCE .....	45
<b>CHAPTER 13: CLOSE OUT .....</b>	<b>47</b>
CLOSE OUT PROCESS .....	48
RETENTION AND MAINTENANCE OF RECORDS.....	48
ACCESS TO RECORDS .....	49
<b>APPENDIX: GLOSSARY OF TERMS.....</b>	<b>50</b>
<b>INDEX.....</b>	<b>56</b>

# Chapter 1: Introduction

Highlights from this chapter:

- What is the purpose of this Guide?
- Who is this Guide designed for?

# Introduction

## What is the purpose of this Guide?

This Guide is intended to be used for the administration of Federal award programs administered by the Office of Grants and Training (G&T) in conjunction with the provisions of the Office of Management and Budget (OMB) circulars and government-wide common rules applicable to grants and cooperative agreements, program guidelines, application kits, special conditions, terms and conditions, G&T information bulletins, and DHS policy, regulations and statutes. Details specific to the OMB Circulars can be found on the OMB website at [www.whitehouse.gov/omb/circulars/](http://www.whitehouse.gov/omb/circulars/). Below is a list of the most commonly used circulars with which grant recipients should become familiar.

### ***Administrative Guidelines:***

**OMB Circular A-102, Grants and Cooperative Agreements with State and Local Governments.** This Circular establishes consistency and uniformity among Federal agencies in the management of grants and cooperative agreements with ***State, local, and Federally recognized Indian tribal governments.***

**OMB Circular A-110, Uniform Administrative Requirements for Grants and Other Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Organizations.** This Circular establishes administrative requirements for Federal grants and agreements awarded to ***commercial organizations, institutions of higher education, hospitals, and other non-profit organizations.***

### ***Cost Guidelines:***

**OMB Circular A-21, Cost Principles for Educational Institutions.** This Circular establishes principles for determining costs applicable to grants, contracts, and other agreements with ***educational institutions.***

**OMB Circular A-87, Cost Principles for State, Local and Indian Tribal Governments.** This Circular establishes principles and standards for determining costs for Federal awards carried out through grants, cost reimbursement contracts, and other agreements with ***State, local and Federally recognized Indian tribal governments.***

**OMB Circular A-122, Cost Principles for Non-Profit Organizations.** This Circular establishes principles for determining costs of grants, contracts and other agreements with ***non-profit organizations.*** It does not apply to colleges and universities, which are covered by Office of Management and Budget (OMB) Circular A-21, "Cost Principles for Educational Institutions"; State, local, and Federally recognized Indian tribal governments, which are covered by OMB Circular A-87, "Cost Principles for State, Local, and Indian Tribal Governments"; or hospitals.

**Code of Federal Regulations, Title 48 Federal Acquisition Regulations Systems, Chapter 1, Part 31, Contract Cost Principles and Procedures.** This part is to be used by

commercial organizations and contains cost principles and procedures for cost analysis and the determination, negotiation and allowance of costs.

***Audit Guidelines:***

**OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations.** This Circular provides requirements regarding audits of ***State, local and tribal governments and non-profit organizations*** (the Single Audit Act), in addition to the circulars for cost principles. This Circular requires that non-Federal entities that expend \$500,000 (effective January 1, 2004) or more of total Federal funds in their fiscal year shall have a single or program-specific audit conducted for that year. Guidance on determining Federal awards expended is provided in **Section 205** of this Circular.

Unless prohibited by law, the costs of audits made in accordance with the provisions of this requirement are allowable charges to Federal awards. The charges may be considered a direct cost or an allocated indirect cost, as determined in accordance with the provisions of applicable OMB cost principles circulars, the Federal Acquisition Regulation (FAR) (48CFR parts 30 and 31), or other applicable cost principles or regulations.

For those organizations not subject to the A-133 requirements, records must still be available and complete for review or audit by appropriate officials or representatives of the Federal agency, pass-through entity, and Government Accountability Office (GAO). These organizations shall have financial and compliance audits conducted by qualified individuals who are organizationally, personally, and externally independent from those who authorize the expenditure of Federal funds to ensure that there is no conflict of interest or appearance of conflict of interest.

The cost of auditing a non-Federal entity that has Federal awards expended of less than \$500,000 per year and is thereby exempted under the A-133 requirement may not charge such costs to their Federal award(s).

***Who is this Guide designed for?***

This document is provided for the use of all recipients and their subrecipients of Federal award programs administered by G&T. This Guide is to serve as the primary reference for financial management and grants administration. Specific organizations and individuals that are to use this Guide include the following:

***Direct Recipients:***

Formula and discretionary recipients receiving funds directly from G&T.

***Subrecipients:***

An individual and/or organization that receives Federal financial or property assistance through the direct recipient of Federal funds. This may include entities receiving funds as a result of formula awards. Units of government and other organizations receiving Federal financial assistance from the State shall adhere to applicable State laws and procedures except where inconsistent with Federal statutes and guidelines. The

circulars and government-wide common rules specific to that organization-type also apply.

Individuals from the above organizations who may use this Guide include, but are not limited to: administrators, financial management specialists, grants management specialists, accountants, and auditors. These individuals are to use the Guide as a financial policy reference in executing their duties under agency-funded programs and projects. Additionally, the document is structured to serve as a training manual for new employees.

This Guide is **not** for the direct use of **contractors**. However, direct recipients should ensure that monitoring of organizations under contract to them is performed in a manner that will ensure compliance with their overall financial management requirements.

***This Guide is intended to be used for fiscal year 2006 and future G&T awards. Any awards made prior to October 1, 2005 must follow the legacy organization's regulations as outlined in the recipient's award terms and conditions.***

### **Order of Precedence**

In determining the relevant standards for the conduct of grant operations, grantees should consider the following, in precedential order:

- Public Laws
- Regulations
- Executive Orders
- OMB Circulars
- Departmental Policy
- Award Terms and Conditions

## Chapter 2: The Application Process

Highlights from this chapter:

- Notice of Funding Availability/Announcements
- Application Review
- Technical Review
- Cost Analysis

# The Application Process

## Notice of Funding Availability/Announcements

A compilation of available assistance programs may be found in the Catalog of Federal Domestic Assistance (CFDA) at [www.cfda.gov](http://www.cfda.gov). G&T grant program announcements can also be found at the DHS/G&T (<http://www.ojp.usdoj.gov/odp/welcome.html>) and Grants.Gov ([www.grants.gov](http://www.grants.gov)) websites or by contacting the Centralized Scheduling Information Desk (CSID) at 1-800-368-6498 or [Askcsid@dhs.gov](mailto:Askcsid@dhs.gov) . The websites will provide you, at minimum, a link to the full application kit and online application system.

***The following kinds of information can be found in the program guidance/solicitation packages for each specific program:***

- Authorization
- Objectives
- Use and Restrictions
- Eligibility - Eligible applicants will be detailed in each program guidance/solicitation package released for funding. Formula funds are generally awarded to the State Administrative Agency (SAA), which may, in turn, subgrant funding to units of local government and nonprofit organizations, based upon statutory authority. (See appropriate specific program guidelines for eligibility.) Discretionary awards may also be awarded to States, units of local government, Indian tribes and tribal organizations, individuals, educational institutions, hospitals, and private nonprofit and private commercial organizations (if legislation allows) at the discretion of DHS/G&T.
- Match Requirements
- Program Description
- Funding Availability
- Program Specific Requirements
- Application Deadlines
- Application Requirements
- Application Forms
- Reporting Requirements

## Application Review

### ***SF 424 Analysis:***

G&T examines information contained in the Application for Federal Assistance (SF 424) to ascertain the following information:

- ***Employer Identification Number (EIN).*** This number includes the Social Security Numbers (SSN) for individuals or employer identification numbers (EIN) for business entities, which are used to identify our customers.
- Whether an applicant holds a ***Federal Debt*** obligation. The SF 424 includes a question about whether there is Federal debt. That question applies to the organization requesting the financial assistance, not the person who signs the

application as the authorized representative of the organization. This kind of debt is defined to include delinquent audit disallowances, loans, and taxes.

- **DUNS number.** All grant applicants must have a Dun & Bradstreet (D&B) Data Universal Numbering System (DUNS) number in order to apply for Federal financial assistance. Organizations may receive a DUNS number at no cost by calling the toll-free DUNS Number request line at 1-866-705-5711. *Individuals* who apply for grant awards or cooperative agreements from the Federal government are *exempt* from this requirement.

### ***Financial Capability and Fiscal Integrity:***

Nongovernmental (non-profit and commercial) organizations that have not previously received DHS/G&T funds or have not had an active award within 3 years must complete the ***Accounting System and Financial Capability Questionnaire***. This form is to be submitted as part of the application package. This Questionnaire may be obtained at <http://www.ojp.usdoj.gov/forms.htm>.

A preliminary assessment of the applicant's financial capability, including the applicant's accounting system and operations, will be completed to ensure that if Federal funds are awarded the funds will be expended in a judicious manner. Where a nongovernmental applicant (except public colleges, universities, and hospitals) has never received an award, the organization's accounting system will be reviewed prior to award or within a reasonable time thereafter to assure its adequacy and acceptability. This review may also apply where known financial or management deficiencies appear to exist. The results of the review will determine the action to be taken by the awarding agency with regard to the award, i.e. additional reporting or monitoring requirements. Where an applicant has had prior awards, outstanding audit issues and delinquent audit, financial, or progress reports must be resolved prior to awarding additional discretionary funds.

The awarding agency will obtain credit reports before making awards to new recipients or to those recipients with poor past performance records. Also, the awarding agency may obtain credit reports on any applicant when there is reason to believe that performance is substandard or there is evidence of financial irregularities. If this preliminary assessment indicates that an applicant may be of higher risk, G&T may impose additional monitoring and/or reporting requirements.

G&T will also take the following information into account when considering the application for award: 1) past grant history, 2) audit reports, and 3) financial and performance report submission.

### **Technical Review**

Awards that are made through a competitive review process will undergo a "peer review". Applications that meet the minimum requirements identified in the program guidance will move forward and be reviewed by a panel(s) of subject matter experts. The subject matter experts will then score and may rank the applications or make recommendations for funding to G&T.

## **Cost Analysis**

G&T may conduct a cost analysis of each project application considered for funding. This cost analysis includes obtaining cost breakdowns, verifying cost data, evaluating specific elements of costs, and examining data to determine the necessity, reasonableness, allowability, allocability, and appropriateness of the proposed cost. The form and extent of such an analysis will be determined by G&T based on the level and type of funding. Each program guidance package will specify when/if a cost analysis will be completed and the type of cost information required.

## Chapter 3: The Award Process

Highlights from this chapter:

- The Award Document
- Acceptance of Award and Conditions
- Types of Financial Assistance: Grant or Cooperative Agreement
- Planning and Implementing Award Programs

# The Award Process

## The Award Document

After completing the internal review process, project applications designated for approval are formally awarded through the issuance of an Award Document.

This document includes:

- Name and address of recipient;
- Date of award;
- Project/performance period;
- Vendor/recipient number;
- Amount of Federal funds;
- Award/agreement number;
- Method of payment; and
- Terms and conditions, as appropriate, that the recipient/subrecipient must meet if the award is accepted.

Notification of the award will be made electronically. Instructions will be provided on how to accept the award. All correspondence concerning the award should refer to the **designated award/agreement number** shown on the Award Document.

## Acceptance of Award and Conditions

The Award Document constitutes the operative document obligating and reserving Federal funds for use by the recipient in executing the program or project covered by the award. Acceptance of a Federal award of funds means that the grantee agrees to abide by all applicable laws, regulations, program guidance and special conditions. This obligation may be voided without further cause if the recipient fails to accept the award in a timely manner.

All awards will include terms and conditions that include requirements concerning compliance with this Guide and compliance with the audit requirements. A number of other standard or special conditions may be attached to the award. ***Recipients are urged to carefully review and understand all terms and conditions of the award prior to award acceptance. Failure to comply with these terms and conditions may result in disallowance of costs and recovery of funds and/or suspension or termination of funds and/or award.***

Commercial Award recipients receiving grant funding from G&T should be aware of the additional special conditions placed on these awards. Commercial organizations must agree not to make a profit as a result of an award and not to charge a management fee for the performance of an award. Also, commercial organizations must agree to comply with the Federal Acquisition Regulations (FAR) cost principles and the administrative requirements of OMB Circular A-110.

If a recipient materially fails to comply with the terms and conditions of an award, whether stated in a Federal statute, regulation, assurance, application, or notice of award, G&T may take one or more of the following actions, as appropriate in the circumstances. This authority also extends to the recipient agency.

1. Temporarily withhold cash payments pending correction of the deficiency by the recipient.
2. Disallow (that is, deny both use of funds and any applicable matching credit for) all or part of the cost of the activity or action not in compliance.
3. Wholly or partly suspend or terminate the current award.
4. Withhold further awards for the project or program.
5. Take other remedies that may be legally available.

## **Types of Financial Assistance: Grant or Cooperative Agreement**

**Grants** are awarded to States, units of local government, or private organizations at the discretion of the awarding agency or on the basis of a formula. Grants are used to support a public purpose.

**Cooperative agreements** are awarded to States, units of local government, or private organizations at the discretion of the awarding agency. Like grants, cooperative agreements are also used to support a public purpose. Cooperative agreements are utilized when substantial involvement is anticipated between the awarding agency and the recipient during performance of the contemplated activity.

## **Planning and Implementing Award Programs**

### ***Planning Prior to Award***

Sound planning practices, both before and after grant awards, are critical to the progress and success of G&T program initiatives. Pre-planning strategies, such as the use of calendars and tickler files and their use through all planning phases, contribute towards program success.

It is imperative that G&T grant applicants not wait until they receive an award to start planning how funds will be spent. Many grant programs require state and local jurisdictions to develop Homeland Security Strategic Plans, as well as descriptions of firefighting and emergency response needs, to which all allocations of grant funds must be tied. (Refer to specific grant program guidelines for requirements.)

All grantees, including subrecipients, should employ pre-planning strategies, to include such activities as threat and vulnerability assessments, needs assessments, and gap analyses prior to making application for a grant award. Based upon the results of these activities, priorities for funding should then be established. Grantees should leverage all relevant funding and resources from multiple sources wherever possible that will support and sustain program efforts. Program budgets should be developed in a manner that maximizes all resources, not restrictive to Federal funding alone, avoids duplication of spending, will help achieve identified priorities, and will account for expenditures.

## Chapter 4: Managing Federal Funds

Highlights from this chapter:

- Financial Management System Requirements
- Recipient and Subrecipient Accounting Responsibilities
- Commingling of Funds
- Monitoring Project Performance
- Conflicts of Interest
- Supplanting

# Managing Federal Funds

## Financial Management System Requirements

All recipients are required to establish and maintain accounting systems and financial records to accurately account for funds awarded to them. These records shall include both Federal funds and all matching funds of State, local, and private organizations, when applicable. State recipients shall expend and account for grant funds in accordance with State laws and procedures for expending and accounting for their own funds. Subrecipients of States shall follow the financial management requirements imposed on them by States, which must comply with the requirements G&T has imposed on the States.

Funds specifically budgeted and/or received for one project may not be used to support another without prior written approval of the awarding agency. Where a recipient's or subrecipient's accounting system cannot comply with this requirement, the recipient or subrecipient shall establish a system to provide adequate fund accountability for each project it has been awarded.

Where the conduct of a program or one of its components is delegated to a subrecipient, the direct recipient is responsible for all aspects of the program, including proper accounting and financial recordkeeping by the subrecipient. Responsibilities include the accounting of receipts and expenditures, cash management, maintenance of adequate financial records, and refunding expenditures disallowed by audits.

## Recipient and Subrecipient Accounting Responsibilities

- **Reviewing Financial Operations** - Direct recipients should be familiar with, and periodically monitor, their subrecipients' financial operations, records, systems, and procedures. Particular attention should be directed to the maintenance of current financial data.
- **Recording Financial Activities** - The subrecipient's award or contract obligation, as well as cash advances and other financial activities, should be recorded in the books of the recipient in summary form. Subrecipient expenditures should be recorded on the books of the recipient or evidenced by report forms duly filed by the subrecipient. Non-Federal contributions applied to programs or projects by subrecipients should likewise be recorded, as should any program income resulting from program operations. All financial records must validate expenditures related to the respective grant(s).
- **Budgeting and Budget Review** - The recipient should ensure that each subrecipient prepares an adequate budget on which its award commitment will be based. The detail of each project budget should be maintained on file by the recipient.
- **Accounting for Non-Federal Contributions** - Recipients will ensure that the requirements, limitations, and regulations pertinent to non-Federal contributions are applied.
- **Audit Requirements** - Recipients must ensure that subrecipients have met the necessary audit requirements contained in this Guide.

- **Reporting Irregularities** - Recipients and their subrecipients shall promptly notify the awarding agency and the Federal cognizant audit agency of any illegal acts or irregularities and of proposed and actual actions, if any. Illegal acts and irregularities include conflicts of interest, falsification of records or reports, and misappropriation of funds or other assets. Should a recipient become aware of any criminal activity related to Federal assistance, these criminal acts should be reported to the appropriate law enforcement agency.
- **Debarred and Suspended Organizations** - Recipients and subrecipients must not award or permit any award at any level to any party that is debarred or suspended from participation in Federal assistance programs.
- **Bonding** - The awarding agency may require adequate fidelity bond coverage where the recipient lacks sufficient coverage to protect the Federal government interest (see OMB Circular A-110, Subpart C, paragraph 21(c) and OMB Circular A-122). Where the conduct of a program or one of its components is delegated to a subrecipient, the direct recipient is responsible for all aspects of the program, including proper accounting and financial recordkeeping by the subrecipient. Responsibilities include accounting for receipts and expenditures, cash management, maintaining adequate financial records, and refunding expenditures disallowed by audits.

## Commingling of Funds

Federal agencies shall not require physical segregation of cash deposits or the establishment of any eligibility requirements for funds that are provided to a recipient. However, the accounting systems of all recipients and subrecipients must ensure that agency funds are not commingled with funds from other awards or Federal agencies. Each award must be accounted for separately. Recipients and subrecipients are prohibited from commingling funds on either a program-by-program or project-by-project basis without prior written approval of the awarding agency.

## Monitoring Project Performance

### ***Recipient Responsibilities:***

A recipient has full responsibility for the conduct of the project or activity supported and for the results achieved. The recipient must monitor the performance of the project to assure adherence to performance goals, time schedules or other requirements as appropriate to the project or the terms of the agreement. The recipient is responsible for monitoring the activities of and pass-through requirements to any subrecipients.

### ***Federal (DHS/G&T) Responsibilities:***

It is DHS/G&T practice to limit involvement between itself and the recipient in the performance of a project to the minimum necessary to achieve program objectives and to ensure conformance with requirements of the grant. The Federal role is that of a partner, where the Government provides the financial assistance and the recipient carries out the project activities. In the case of a cooperative agreement, substantial involvement is expected between the Federal agency and the State, local government, or other recipient when carrying out the activity contemplated in the agreement.

Monitoring is a process whereby the programmatic progress and financial and business management aspects of a financial assistance award are reviewed by assessing information gathered from program and financial reports, site visits, teleconferences, and other means. DHS/G&T requires financial assistance recipients to have adequate management systems to ensure that project objectives are met and funds are spent and accounted for properly. To the extent possible, financial assistance award monitors rely on the management systems of the financial assistance recipients to meet project objectives, comply with award terms and conditions, and account for funds.

## **Conflicts of Interest**

To avoid conflicts of interest, personnel and other officials connected with agency funded programs shall adhere to the following requirements:

No official or employee of a State or unit of local government or a non-governmental recipient/subrecipient shall participate personally through decisions, approval, disapproval, recommendation, the rendering of advice, investigation, or otherwise in any proceeding, application, request for a ruling or other determination, contract, award, cooperative agreement, claim, controversy, or other particular matter in which award funds (including program income or other funds generated by Federally funded activities) are used, where to his/her knowledge, he/she or his/her immediate family, partners, organization other than a public agency in which he/she is serving as an officer, director, trustee, partner, or employee, or any person or organization with whom he/she is negotiating or has any arrangement concerning prospective employment, has a financial interest, or has less than an arms-length transaction.

In the use of agency project funds, officials or employees of State or local units of government and non-governmental recipient/subrecipients shall avoid any action that might result in, or create the appearance of:

- Using his or her official position for private gain;
- Giving preferential treatment to any person;
- Losing complete independence or impartiality;
- Making an official decision outside official channels; or
- Affecting adversely the confidence of the public in the integrity of the government or the program. For example, where a recipient of federal funds makes sub-awards under any competitive process and an actual conflict or an appearance of a conflict of interest exists, the person for whom the actual or apparent conflict of interest exists should recuse himself or herself not only from reviewing the application for which the conflict exists, but also from the evaluation of all competing applications.

Violations of the conflict of interest standards may result in criminal, civil, or administrative penalties.

## **Supplanting**

Recipients of G&T funds shall not replace funding appropriated from State and local governments with their Federal grant funding. It is the purpose of these grants to increase the overall amount of resources available to any G&T funded organization in order to bolster preparedness and to increase services and opportunities. Current levels

of activities or programs funded by State, local or non-governmental entity resources should only be increased by receipt of Federal funding. Recipients therefore must ensure that they do not reduce the current overall level of funding support to preparedness missions, absent exigent circumstances.

For example, if a State pays the salaries of three intelligence analysts, it cannot begin to pay the salary of one of them with Federal grant funding. It could, however, hire a fourth analyst.

Potential supplanting will be the subject of application review, as well as pre-award review, post-award monitoring, and audit. If there is a potential presence of supplanting, the applicant or grantee will be required to supply documentation demonstrating that the reduction in non-Federal resources occurred for reasons other than the receipt or expected receipt of Federal funds.

A confirmation during the application process may be requested by the awarding agency or recipient agency stating that Federal funds will not be used to supplant State or local funds.

## Chapter 5: Payments

Highlights from this chapter:

- Request for Advance or Reimbursement
- Withholding of Funds
- Cash Management Improvement Act of 1990
- Interest

# Payments

The method used to request grant funds may be different depending on the grant program. Information on how to access grant funds is provided to grant recipients in the program guidance and/or post award instructions. For assistance in determining the method to be used for payment requests, please contact the Office of Grant Operations at 1-866-9ASK-OGO or ASK-OGO@DHS.GOV.

## Request for Advance/Reimbursement

Recipient organizations generally request funds based upon immediate disbursement requirements. Funds will not be paid in a lump sum, but rather disbursed over time as project costs are incurred or anticipated. Recipients should time their drawdown requests to ensure that Federal cash on hand is the minimum needed for disbursements to be made immediately or within a few days. Beginning with fiscal year 2005 funds, recipients may elect to drawdown funds up to 120 days prior to expenditure/disbursement. G&T strongly encourages recipients to draw down funds as close to expenditure as possible to avoid accruing interest.

Fund requests from subrecipients create a continuing cash demand on award balances of the State. The State should keep in mind that idle funds in the hands of subrecipients will impair the goals of sound cash management. All recipients must develop procedures for the disbursement of funds to ensure that Federal cash on hand is kept at a minimal balance.

## Withholding of Funds

G&T may withhold payments to a recipient organization after proper notification or opportunity to remedy, by demonstrating any of the following:

1. Unwillingness or inability to attain program or project goals or to establish procedures that will minimize the time elapsing between cash drawdowns and expenditures;
2. Inability to adhere to guideline requirements or special conditions;
3. Improper award and administration of subawards or contracts; and
4. Inability to submit reliable and/or timely reports.

## Cash Management Improvement Act of 1990

The Cash Management Improvement Act (CMIA) provides the general rules and procedures for the efficient transfer of Federal financial assistance between the Federal government and the States. Under this Act, States are no longer exempt from payment of interest to the Federal government resulting from drawing down funds prior to the need to pay off obligations incurred. States must pay interest in the event that the States draw down funds before the funds are needed to pay for program expenses.

**Please note:** Although recipients may draw down funds up to 120 days in advance of expenditure, **State grantees are still subject to the interest requirements of the**

CMIA and its implementing regulations at 31 C.F.R. Part 205. Interest under CMIA will accrue from the time Federal funds are credited to a State account until the time the State pays out the funds to a subgrantee or otherwise expends for program purposes. Recipients should request funds based on an immediate cash needs basis.

## **Interest**

Recipients and subrecipients shall minimize the time elapsing between the transfer and disbursement of funds.

1. A State, its subrecipient and any agency or instrumentality of a State, including State institutions of higher education and State hospitals, but not political subdivisions of a State (cities, towns, counties, and special districts created by State law) SHALL NOT be held accountable for interest earned on grant money pending its disbursement for program purposes. This refers to formula grant programs where subawards are made to local jurisdictions. Subrecipients under formula grant programs are held accountable for interest earned on advances.
2. Tribal organizations SHALL NOT be held accountable for interest earned pending their disbursement by such organizations.
3. All local units of government (political subdivisions of a State, including cities, towns, counties and special districts created by State law) shall account for interest earned on Federal funds. Local units of government may keep interest earned on Federal grant funds up to \$100 PER FEDERAL FISCAL YEAR. This maximum limit is not per award; it is inclusive of all interest earned as a result of all Federal grant program funds received per year.
4. Nonprofit and commercial organizations shall account for interest earned on Federal funds. Nonprofit organizations may keep interest earned on Federal grant funds up to \$250 PER FEDERAL FISCAL YEAR. This maximum limit is not per award; it is inclusive of all interest earned as a result of all Federal grant program funds received per year.

For G&T grants, interest earned, in excess of the amounts stated above, must be remitted to the United States Department of Health and Human Services, Division of Payment Management Services, P.O. Box 6021, Rockville, MD 20852.

For Assistance to Firefighters Grants (AFG) grants, interest should be remitted to the FEMA-Accounting Services Division, Disbursements and Receivables Branch, 500 C Street, S.W., Room 723, Washington, D.C. 20472.

## Chapter 6: Obligation and Expenditures

Highlights from this chapter:

- Obligation of Funds
- Period of Availability
- Expenditure of Funds
- Suspension and Termination

# Obligation and Expenditures

## Obligation of Funds

Obligations are a legal liability to pay, under a grant, subgrant, and/or contract, determinable sums for services or goods incurred during the grant period. This includes, but is not limited to, amounts of orders placed, contracts and grants awarded, services received and similar transactions that require payment by the recipient during the same or a future period.

## Period of Availability

The award period is the period of time when Federal funding is available for obligation by the recipient. The recipient may charge to the grant only allowable costs resulting from obligations incurred during the funding period and any pre-award costs authorized by G&T. An obligation occurs when funds are encumbered, such as in a valid purchase order or requisition to cover the cost of purchasing an authorized item on or after the begin date and up to the last day of the grant period in the award. Any funds not properly obligated by the recipient within the grant award period will lapse and revert to G&T. The obligation deadline is the last day of the grant award period unless otherwise stipulated. The obligation period is the same as the award period listed on the award document. No additional obligations can be incurred after the end of the grant.

*Example: If the award period is 10/1/04 to 9/30/05, the obligation deadline is 9/30/05.*

## Expenditure of Funds

Recipients who have properly obligated funds by the end of the award period will have 90 days in which to liquidate (expend) these funds. Any funds not liquidated at the end of the 90-day period will lapse and may revert to G&T, unless an adjustment extending the liquidation period has been approved. Refer to Chapter 8 for more information regarding extensions.

*Example: If the award period is 10/1/2004 to 9/30/2005, then all funds obligated by 9/30/2005 must be liquidated/expended by 12/29/2005.*

## Suspension and Termination

G&T may terminate any project, in whole or in part, for the convenience of the Government or when a recipient materially fails to comply with the terms and conditions of an award. This includes unauthorized use of payment access codes by someone other than the grantee of record, or when the recipient and G&T agree to do so. In the event that the decision has been made to terminate a project, G&T will:

1. Notify the recipient in writing of its decision;
2. Specify the reason; and
3. Afford the recipient/subrecipient a reasonable time to offer a remedy or to terminate project operations.

A project that is terminated will be subject to the same requirements regarding audit, recordkeeping, and submission of reports as a project that runs for the duration of the project period. Upon notification, no new obligations may be made against the award.

## Chapter 7: Grant Reporting

Highlights from this chapter:

- Financial Reporting
- Programmatic Reporting

# Grant Reporting

G&T requires award recipients to submit both financial and program reports. These reports describe the status of the funds, the status of the project, a comparison of actual accomplishments to the objectives, the reason(s) goals have not been met, and/or other pertinent information. The specific requirements, reporting periods and submission deadlines are detailed in the program guidance and/or terms and conditions of the award. ***Future awards, fund drawdowns, and modification approvals may be withheld if financial and program reports are delinquent.***

## Financial Reporting

Generally, G&T requires grant recipients to submit a quarterly Financial Status Report (SF 269a) for each active grant award. These reports are due 30 days after the end of the calendar quarter. Financial reporting requirements may vary for G&T grant programs; therefore, for specific reporting instructions on a given grant program, please refer to the program guidance for information regarding the report to be submitted, the frequency of reporting and the deadline for submission of the report.

For those recipients required to submit the SF269a quarterly Financial Status Report, this report must be submitted on-line using the Grants Management System. The link to submit this report is <https://grants.ojp.usdoj.gov/>. For assistance using this system, recipients may contact the OJP GMS Help Desk at 888-549-9901 or at [gms.helpdesk@usdoj.gov](mailto:gms.helpdesk@usdoj.gov). ***As of January 1, 2006 paper copies of these forms will no longer be accepted.***

## Programmatic Reporting

All G&T grant programs require that the recipient report on the performance and progress of grant activities. Reporting requirements may vary in format and in time frame, so please refer to the specific guidance for each program for full details on the required program report(s).

For those recipients required to submit the semi-annual Categorical Assistance Progress Report (CAPR), this report must be submitted on-line using the Grants Management System. The link to submit this report is <https://grants.ojp.usdoj.gov/>. For assistance using this system, recipients may contact the OJP GMS Help Desk at 888-549-9901 or at [gms.helpdesk@usdoj.gov](mailto:gms.helpdesk@usdoj.gov). ***As of January 1, 2006 paper copies of these reports will no longer be accepted.***

## Chapter 8: Adjustments to Awards

Highlights from this chapter:

- Modifications and Revisions (including Grant Adjustment Notices)
- Notification of Changes
- Types of Adjustments

# Adjustments to Awards

## Modifications and Revisions (including Grant Adjustment Notices)

All requests for programmatic and/or administrative changes must be submitted in a timely manner by the recipient/subrecipient. All requests for changes to the approved award shall be carefully reviewed by the applicable authority for both consistency with this Guide and their contribution to the project goals and objectives.

### Notification of Changes

All recipients must give notification in writing to G&T of events or proposed changes that may require an adjustment/notification. In requesting an adjustment, the recipient must set forth the reasons and basis for the proposed change and any other data deemed helpful for G&T review. Recipient requests will be reviewed by G&T and approval of these changes, if granted, will be provided in writing. ***Requests for adjustments will be considered only if the reporting requirements are current and terms and conditions have been met at the time the request for the adjustment is made.***

### Types of Adjustments:

- Change of Address - Recipients are required to notify G&T of changes to their mailing address.
- Changes in Award Period - Recipients may request an extension of the award/obligation and expenditure period. Written requests should be at least 90 calendar days before the end date of the award. A narrative justification must be submitted with the project or program extension request on agency letterhead. Complete details must be provided, including the justification and the extraordinary circumstances that require the proposed extension, and a certification that there are adequate funds remaining to support the extension. Explain the effect of a denial of the request on the project or program.
- Changes in Scope - Change in the scope of the programmatic activities or purpose of the project.
- Change in project site.
- Changes that increase or decrease the total cost of the project.
- Change in approved budget categories in excess of 10 percent of the total award amount - Movement of dollars between approved budget categories is allowed up to 10 percent of the total budget cost (total award amount) as last approved by G&T, provided there is no change in project scope. When the cumulative changes exceed 10 percent of the total award amount (includes the initial award plus the supplements) or change the scope of the project, prior approval from G&T is required. This 10 percent rule applies to awards over \$100,000; however, if the total award is equal to or less than \$100,000, and the scope of the project doesn't change, prior approval is not required unless otherwise required in the program guidance or award documents.
- Change in or temporary absence of the project manager/director.
- Transfer of project.
- Successor in interest and name change agreements.
- Addition of an item to the project budget requiring prior approval.

- Retirement of special conditions, if required.
- Changes in key personnel, if any are specified by the special conditions.
- Change of State Administrative Agency (SAA) - Should the Governor of a state elect to change the SAA during the grant period, the current SAA must close-out the grant(s) that are transferring to the new SAA prior to any funds being transferred to the newly designated SAA. The close-out information must include, at minimum, a final Financial Status Report (SF-269a) and a final program report. It is G&T policy that these funds will not be awarded to the newly designated SAA prior to close-out of the original award. States are responsible for working with their vendors and/or subrecipients to obtain final expenditure reports, invoices, payment requests, etc. in a timely manner in order to assist in the transfer of funds to the new SAA. Once the close-out information has been submitted to G&T, the newly designated SAA will be permitted to apply for the remaining funds through the Grants Management System.

## Chapter 9: Other Program Funds

Highlights from this chapter:

- Program Income
- Requirements for Match or Cost Sharing

# Other Program Funds

## Program Income

Program income is gross income earned by the recipient that is directly generated by a supported activity or earned as a result of the program. Program income includes, but is not limited to, income from fees for services performed, the use or rental of real or personal property acquired under Federally funded projects, the sale of commodities or items fabricated under an award, license fees and royalties on patents and copyrights, and interest on loans made with award funds. For example, if the purpose of the grant is to conduct conferences, any training fees that are generated would be considered program income. Interest earned on advances of Federal funds is **not** program income.

### ***Accounting for and Reporting Program Income***

Program income earned during the project period shall be retained by the recipient and, in accordance with OMB regulations or the terms and conditions of the award, shall be used and accounted for in one or more of the following ways.

1. Added to funds committed to the project by the Federal awarding agency and recipient and used to further eligible project or program objectives.
2. Used to finance the non-Federal share of the project or program, if applicable.
3. Deducted from the total project or program allowable cost in determining the net allowable costs on which the Federal share of costs is based.

Program income may be used to supplement project costs or reduce project costs, or may be refunded to the Federal government. Program income may only be used for allowable program costs and must be expended prior to additional drawdowns.

### ***Use and Disposition of Program Income***

Unless specified by G&T, program income should be used as earned and expended as soon as possible. If the cost is allowable under the Federal grant program, then the cost would be allowable using program income. If program income earned on a discretionary grant during the grant period remains at the end of the grant period, the recipient should request a no-cost extension of the grant period to provide the recipient with ample time to expend the program income for allowable project purposes. If there is no special condition on the award concerning the accounting for program income earned after the funding period, then such program income can be used at the discretion of the recipient. The Federal portion of program income must be accounted for up to the same ratio of Federal participation as funded in the project or program. For example:

1. A discretionary project funded with 100 percent Federal funds must account for and report on 100 percent of the total program income earned. If the total program income earned was \$20,000, the recipient must account for and report the \$20,000 as program income on the Financial Status Report.
2. If a recipient was funded by formula funds at 75 percent Federal funds and 25 percent non-Federal funds and the total program income earned by the grant

was \$100,000, \$75,000 must be accounted for and reported, by the recipient, as program income on the Financial Status Report.

Direct recipients of formula grants will be responsible for requiring subrecipients to comply with program income guidelines.

*For additional information on Program Income please refer to the appropriate OMB Circular (A-102 or A-110)*

## Requirements for Matching or Cost Sharing

Funds provided for a match must be used to support a Federally funded project and must be in addition to, and therefore supplement, funds that would otherwise be made available for the stated program purpose. Match is restricted to the same use of funds as allowed for the Federal funds.

Matching contributions need not be applied at the exact time or in proportion to the obligation of the Federal funds unless stipulated by legislation. However, the full matching share must be obligated by the end of the period for which the Federal funds have been made available for obligation under an approved program or project.

Sources of the match can either be a **cash** match **or** an **in-kind** match unless specified in the program guidance, regulation or statute.

**Cash Match** includes cash spent for project-related costs. Allowable cash match must include those costs that are allowable with Federal funds with the exception of the acquisition of land, when applicable. Cash match may be applied from the following sources:

1. Funds from states and local units of government that have a binding commitment of matching funds for programs or projects, or
2. Funds from the following:
  - Housing and Community Development Act of 1974, 42 USC §5301, et seq. (subject to the applicable policies and restrictions of the Department of Housing and Urban Development).
  - Appalachian Regional Development Act of 1965, 40 USC §214.
  - Equitable Sharing Program, 21 USC §881(e) (current guidelines developed by the DOJ Asset Forfeiture Office apply). Forfeited assets used as match from the Equitable Sharing Program would be adjudicated by a Federal court.
  - Funds contributed from private sources.
3. Program income and the related interest earned on that program income generated from projects, provided they are identified and approved prior to making an award, or
4. Funds earned from seized assets and forfeitures (adjudicated by a State court, as State law permits), or

5. Funds appropriated by Congress for the activities of any agency of a Tribal government or the Bureau of Indian Affairs performing law enforcement functions on Tribal lands, or

6. Sources otherwise authorized by law.

Except as noted above, Federal funds may not be used for match purposes.

***In-kind Match*** includes, but is not limited to, the valuation of in-kind services. “In-kind” is the value of something received or provided that does not have a cost associated with it. For example, if in-kind match is permitted by law, then the value of donated services could be used to comply with the match requirement.

**Recordkeeping:** Recipients and their subrecipients must maintain records that clearly support the source, the amount, and the timing of all matching contributions. In addition, if a program or project has included within its approved budget contributions that exceed the required matching portion, the recipient must maintain records of them in the same manner as it does the awarding agency funds and required matching shares. The direct recipient has primary responsibility for subrecipient compliance with requirements.

**Waiver of Match Requirement:** In accordance with 48 USC §1469a, congressional declaration of a policy regarding insular areas, the awarding agency, in its discretion, shall waive any requirement for matching funds otherwise required by law to be provided by the certain insular areas. This waiver applies to ALL awards made to American Samoa, Guam, the Virgin Islands, and Northern Mariana Islands.

## Chapter 10: Costs and Expenditures

Highlights from this chapter:

- Allowable Costs
- Unallowable Costs
- Costs Requiring Prior Approval

# Costs and Expenditures

## Allowable Costs

Allowable costs are those costs identified in the circulars, as noted below, and in the grant program's authorizing legislation. In addition, costs must be reasonable, allocable, necessary to the project, and comply with the funding statute requirements. Recipients should refer to the program guidelines to determine what program costs are allowable for that specific program. It is important to note that costs that are allowable under one G&T program may be specifically prohibited under another. Additionally, allowable items may change from one fiscal year to another, so it is important to verify allowable costs with Program Guidance specific to the fiscal year funding.

Please note, grantees generally are not required to comport with the restrictions of the Buy American Act (41 U.S.C. 10a). However, grants authorized under the Stafford Act, including the *Emergency Management Performance Grant*, must follow these standards. The Buy American Act requires that all materials purchased be produced in the United States, unless such materials are not available, or such a purchase would not be in the public interest.

Applicable Cost Principles:

[OMB Circular A-21](#) "Cost Principles for Educational Institutions"

[OMB Circular A-87](#) "Cost Principles for State, Local, and Indian Tribal Governments"

[OMB Circular A-122](#) "Cost Principles for Nonprofit Organizations"

[Code of Federal Regulations, Title 48 Federal Acquisition Regulations Systems, Part 31](#)  
"Contract Cost Principles and Procedures"

## Equipment

For G&T programs that include the purchase of equipment, recipients are encouraged to review the Interagency Board's (IAB) Standardized Equipment List (SEL) and the Authorized Equipment List (AEL). These lists maybe be found on the Responder Knowledge Base (RKB) website at <http://www.rkb.mipt.org>. If State agencies and/or local governments have questions concerning the eligibility of equipment not specifically addressed in the AEL, they should contact their Program Manager or Preparedness Officer for clarification.

## Disposition or Recovery of Federally Owned Assets

A State will dispose of equipment acquired under a grant by the State in accordance with State laws and procedures. All other grantees and subgrantees shall dispose of equipment as follows:

1. Items of equipment with a current per unit fair market value of less than \$5,000 may be retained, sold or otherwise disposed of with no further obligation to the awarding agency.

2. Items of equipment with a current per unit fair market value greater than \$5,000 may be retained or sold and the awarding agency shall have a right to an amount calculated by multiplying the current market value or proceeds from sale by the awarding agency's share of the equipment.

To remit payments, award recipients should contact the Office of Grant Operations (ASK-OGO@DHS.GOV or 1-866-9ASK-OGO) for further instructions.

### **Consultant Rates**

Compensation for individual consultant services is to be reasonable and consistent with the amount paid for similar services in the market place. Consideration can be given to compensation, including fringe benefits, for those individuals whose employers do not provide the same. Time and effort reports are required for consultants. Competitive bidding for consultant services is encouraged.

### **State and Local Sales Taxes**

State and local sales taxes are generally allowable costs, unless the tax is levied solely on Federal programs or Federal funding.

### **Indirect Costs**

Indirect costs are costs of an organization that are not readily assignable to a particular project, but are necessary to the operation of the organization and the performance of the project. The cost of operating and maintaining facilities, depreciation, and administrative salaries are examples of the types of costs that are usually treated as indirect.

In order to be reimbursed for indirect costs, a recipient must first obtain an approved indirect cost rate. To do this, the recipient must prepare an indirect cost rate proposal and submit it to the cognizant Federal agency. The cognizant Federal agency is assigned by OMB or is determined based on the preponderance of Federal dollars received by the recipient, or which agency has awarded the most funds. If an indirect cost proposal for recovery of actual indirect costs is not submitted to the cognizant Federal agency within three months of the start of the award period, indirect costs will be irrevocably lost for all months prior to the month that the indirect cost proposal is received. This requirement is effective for all awards.

If a recipient has a Federally approved indirect cost rate agreement, G&T will accept any current indirect cost rate or allocation plan previously approved for a recipient by any Federal awarding agency on the basis of allocation methods substantially in accord with those set forth in the applicable cost circulars. Approving rates for subrecipients is the responsibility of the direct recipient. Per the OMB guidelines, G&T does not approve indirect cost rates beyond the direct recipient level. For information on how to obtain an approved indirect cost rate, direct recipients should contact the Office of Grant Operations at 1-866-9ASK-OGO or ASK-OGO@DHS.GOV.

## **Indirect Costs versus Management and Administrative (M&A) Costs**

**Indirect costs** are defined as costs that are incurred for common or joint objectives and therefore cannot be identified readily and specifically with a particular award/project, but contribute to the ability of the recipient to support projects and programs and sustain the daily operations of the organization. Indirect costs are not incurred specifically from the actual performance of the activities under a particular award. Indirect costs are charged based on an approved rate and applicable base, which encompasses total organizational activity.

Indirect costs may include:

- Depreciation
- Rent
- Telephone
- Postage
- Printing
- Other expenses that benefit all programs and functions of an organization.

**Management and Administrative costs** are direct costs that are incurred to administer a particular program/award. M&A costs are identifiable and unique to each program/award and are charged based on the activity performed for that particular project.

M&A costs may include:

- Salaries of full-time or part-time staff or contractors/consultants to assist with the management of the program
- Hiring of full-time or part-time staff or contractors/consultants to assist with the implementation and administration of the program
- Travel expenses
- Meeting-related expenses

## **Food and Beverages**

Food and/or beverage expenses provided by recipients are allowable costs if: (1) the food and/or beverages are provided to participants at training sessions, meetings, or conferences that are allowable activities under the particular G&T program guidelines; and (2) Expenses incurred for food and/or beverages and provided at training sessions, meetings, or conferences satisfy the following tests: (a) the cost of the food and/or beverages provided is considered to be reasonable; (b) the food and/or beverages provided are subject of a work-related event; (c) participation by all participants is mandatory; and (d) the food and/or beverages provided are not related directly to amusement and/or social events. (Any event where alcohol is being served is considered a social event; therefore, costs associated with that event are not allowable). In the event food/meal(s) are being provided, the amount charged for per diem must be reduced accordingly.

## **Software development**

Software development costs are allowable and may be expended in the period incurred with no dollar limitation.

## **Maintenance contracts**

The cost of an equipment maintenance agreement is allowable for the period of time that covers the grant project period. Any portion of the contract that extends beyond the grant period may not be charged to the grant award using Federal or matching funds. For example, if the grant project period is one year and the maintenance agreement is for three years, only the cost associated with the first year of the agreement would be allowable. The grantee would have to prorate the cost of the agreement to cover only the grant project period.

## **Warranty costs**

Warranty costs (extensions) on equipment providing extended coverage for parts, labor and repair, above and beyond the term of the original manufacturer's warranty, are allowable if the cost of the warranty is included as part of the acquisition cost. Acquisition cost means the cost of the asset including the cost to put it in place. Acquisition cost for equipment, for example, means the net invoice price of the equipment, including the cost of any modifications, attachments, accessories, or auxiliary apparatus necessary to make it usable for the purpose for which it is acquired.

## **Unallowable Costs**

In addition to the applicable OMB cost principles, recipients should refer to the program guidelines to determine what program costs are not allowed for that specific program. Costs that are unallowable under one G&T program may be allowed under another. Costs generally unallowable under Federal grants are as follows:

### **Land Acquisition**

Land acquisition costs are unallowable unless otherwise noted in grant guidance.

### **Compensation of Federal Employees**

Salary payments, consulting fees, or other compensation of full-time Federal employees are unallowable costs.

### **Travel of Federal Employees**

Costs of transportation, lodging, subsistence, and related travel expenses of G&T employees are unallowable charges. Travel expenses of other Federal employees for advisory committees or other program or project duties or assistance are allowable if they have been:

1. Approved by the Federal employee's Department or Agency; and

2. Included as an identifiable item in the funds budgeted for the project or subsequently submitted for approval.

### **Bonuses or Commissions**

The recipient or subrecipient is prohibited from paying any bonus or commission to any individual or organization for the purpose of obtaining approval of an application for award assistance. Bonuses to officers or board members of profit or non-profit organizations are determined to be a profit or fee and are unallowable.

### **Lobbying**

All recipients and subrecipients must comply with the provisions of the government-wide Common Rule on Restrictions on Lobbying, as appropriate.

### **Fund Raising**

Costs of organized fund raising, including financial campaigns, endowment drives, solicitation of gifts and bequests, and similar expenses incurred solely to raise capital or obtain contributions, may not be charged either as direct or indirect costs against the award. Neither the salary of persons engaged in such activities nor indirect costs associated with those salaries may be charged to the award, except insofar as such persons perform other program related activities.

An organization may accept donations (i.e., goods, space, services) as long as the value of the donations is not charged as a direct or indirect cost to the award. The donation must be supported with source documentation.

A recipient may also expend funds, in accordance with approved award terms, to seek future funding sources to expand the project, but not for the purpose of raising funds to finance related or complementary project activities.

Nothing in this section should be read to prohibit a recipient from engaging in fund raising activities as long as such activities are not financed by the Federal or non-Federal portion of award funds.

### **Conferences and Workshops**

Unallowable costs include:

- Entertainment;
- Sporting events;
- Visa fees;
- Passport charges;
- Tips;
- Bar charges/Alcoholic beverages;
- Laundry charges; and
- Lodging costs in excess of Federal per diem.

## Costs Requiring Prior Approval

Written approval is required for those costs specified in OMB Circulars A-21, A-87, and A-122 as “Costs Allowable With Approval of Awarding Agency” or costs that contain special limitations.

Where prior approval is required, G&T will be the approval authority for all discretionary recipients and for the State when it is the direct recipient. Where prior approval authority for subrecipients is required, it will be vested in the State unless specified as being “RETAINED BY THE FEDERAL AWARDING AGENCY,” as identified below.

Subrecipient requests for G&T approval should be submitted through the State for a formula award.

The intention of G&T is not to require approval of all changes within the listed cost categories, but only for those aspects or elements that specifically require prior approval.

### Types of Costs Requiring Prior Approval

The following is a list of costs that require prior approval:

- **Construction** - The use of G&T funds for construction is generally prohibited, except as outlined in the specific program guidelines (see program specific guidelines for details). Written approval must be provided by G&T prior to the use of any G&T funds for construction or renovation.
- **Preagreement Costs** - Costs incurred prior to the start date of the award may be charged to the project only if the recipient receives prior approval from G&T. Prior approval is required for costs incurred before the date of the subaward period and costs may be charged to the project only if the award or subaward application specifically requests support for preagreement costs. States may approve preagreement costs for subrecipients if incurred subsequent to the beginning of the Federal fiscal year of award.
- **Proposal Costs** - Unless specifically outlined in program guidance as allowable without prior approval, costs to projects for preparing proposals for potential Federal awards require PRIOR APPROVAL for: (1) the obligation or expenditure of funds; or (2) the performance or modification of an activity under an award/subaward project, where such approval is required.
- **Audit Costs** - Audit costs for audits not required or performed in accordance with OMB Circular A-133 are unallowable. If the grantee did not expend \$500,000 or more in Federal funds in its fiscal year, but contracted with a certified public accountant to perform an audit, these costs may not be charged to the grant.
  - Unless prohibited by law, the cost of audits made in accordance with the provisions of this requirement are allowable charges to Federal awards. The charges may be considered a direct cost or an allocated indirect cost, as determined in accordance with the provisions of applicable OMB cost

principles circulars, the Federal Acquisition Regulation (FAR) (48CFR parts 30 and 31), or other applicable cost principles or regulations.

- The cost of auditing a non-Federal entity which has Federal awards expended of less than \$500,000 per year and is thereby exempted under the A-133 requirement may not charge such costs to their Federal award(s).
- **Interest Expense** - Interest on debt incurred for: (a) acquisition of equipment and buildings; (b) building construction; (c) fabrication; (d) reconstruction; and (e) remodeling is an allowable cost with prior approval. This interest applies only to buildings completed on or after 10/1/80 for State and local units of government and 9/29/95 for non-profit organizations.
- **Foreign Travel** - Direct charges for foreign travel costs are allowable only when the travel has prior approval of G&T. Foreign travel is defined as any travel outside of Canada and the United States and its territories and possessions. However, for organizations located in foreign countries, the term "foreign travel" means travel outside that country.

Note: Indirect charges for foreign travel are allowable without prior approval of G&T when: (a) included as part of a Federally approved indirect cost rate; and (b) such costs have a beneficial relationship to the project. Each separate foreign trip must be approved.

Recipients must comply with the provisions of the Fly America Act (49 USC § 40118). The Fly America Act requires travelers performing U.S. Government-financed foreign air travel to use U.S. flag air carriers to the extent that such service is available. Foreign air carriers may be used only in specific instances, such as when a U.S. flag air carrier is unavailable, or use of U.S. flag air carrier service will not accomplish the mission. If a foreign air carrier is used for any part of foreign travel, the recipient must maintain supporting documentation in the grant files available and specifically identified for review during an audit.

Requests must be in writing and justified with an explanation to permit review of the allowability. They may be submitted:

1. Through inclusion in the budget or other components of an award or subaward application; or
2. As a separate written request to the appropriate authority as described above.

## Chapter 11: Procurement

Highlights from this chapter:

- Procurement Standards
- Sole Source Procurement (Non-Competitive)

# Procurement

There are times when it may be necessary to procure goods and/or services in order to accomplish the goals of a program. For example, it may be necessary to purchase equipment or subcontract for services that the recipient does not have the required in-house expertise to perform.

## Procurement Standards

- **General** - A State shall follow the same policies and procedures it uses for procurement from its non-Federal funds. The State shall ensure that every purchase order or other contract includes any clauses required by Federal statutes and executive orders and their implementing regulations. Subrecipients of States shall follow the procurement requirements imposed upon them by the States. Other recipients and subrecipients will follow the appropriate OMB Circular (OMB Circular A-110 or OMB Circular A-102).
- **Standards** - Recipients and subrecipients shall use their own procurement procedures and regulations, provided that the procurement conforms to applicable Federal law and standards.
- **Adequate Competition** - All procurement transactions, whether negotiated or competitively bid and without regard to dollar value, shall be conducted in a manner so as to provide maximum open and free competition. All sole-source procurements in excess of \$100,000 must receive prior written approval of the awarding agency. Interagency agreements between units of government are excluded from this provision.
- **Non-competitive Practices** - The recipient/subrecipient shall be alert to organizational conflicts of interest or non-competitive practices among contractors that may restrict or eliminate competition or otherwise restrain trade. Contractors that develop or draft specifications, requirements, statements of work, and/or Requests for Proposals (RFP) for a proposed procurement shall be excluded from bidding or submitting a proposal to compete for the award of such procurement. Any request for exemption must be submitted in writing to the awarding agency.

## Sole Source Procurement (Non-Competitive)

All non-state procurement transactions shall be conducted in such a manner that provides, to the maximum extent practical, open and free competition. However, should a recipient elect to award a contract without competition, sole source justification may be necessary. Justification must be provided for non-competitive procurement and should include a description of the program and what is being contracted for, an explanation of why it is necessary to contract noncompetitively, time constraints and any other pertinent information. G&T will approve sole-source procurements for direct recipients only. Subrecipients must obtain approval from the primary recipient. If the primary recipient's

regulations require approval at a lower dollar threshold than identified above, the subrecipient should abide by the primary recipient's requirements.

## Chapter 12: Audits

Highlights from this chapter:

- Audit Requirements for States, Local Governments, and Non-Profit Organizations
- Audits of Commercial/For-Profit Organizations
- Audits of Subrecipients
- Distribution of Reports
- Technical Assistance

# Audits

## Audit Requirements for States, Local Governments, and Non-Profit Organizations

Grantees and subrecipients are responsible for obtaining audits in accordance with OMB Circular A-133, "Audits of States, Local Governments, and Non-Profit Organizations". States, local governments or private, non-profit organizations that expend \$500,000 or more in Federal awards in a fiscal year are required to have an audit performed.

- The audits shall be completed by an independent auditor in accordance with generally accepted government auditing standards covering financial audits.
- Audits are due no later than nine (9) months after the close of each fiscal year during the term of the award.
- Grantee audit reports will be distributed by the Federal Audit Clearinghouse to the organization's Federal Cognizant Agency for review and resolution of any findings.
- Grantees are responsible for follow-up and corrective action on all audit findings.

Awards are subject to conditions of fiscal, program, and general administration to which the recipient expressly agrees. Accordingly, the audit objective is to review the recipient's administration of funds and required non-Federal contributions for the purpose of determining whether the recipient has:

1. Established an accounting system integrated with adequate internal fiscal and management controls to provide full accountability for revenues, expenditures, assets, and liabilities. This system should provide reasonable assurance that the organization is managing Federal financial assistance programs in compliance with applicable laws and regulations.
2. Prepared financial statements that are presented fairly, in accordance with generally accepted accounting principles.
3. Submitted financial reports (which may include Financial Status Reports, Cash Reports, and Claims for Advances and Reimbursements), that contain accurate and reliable financial data, and are presented in accordance with the terms of applicable agreements.
4. Expended Federal funds in accordance with the terms of applicable agreements and those provisions of Federal law or regulations that could have a material effect on the financial statements or on the awards tested.

Independent auditors should follow the requirements prescribed in OMB Circular A-133. If the auditor becomes aware of illegal acts or other irregularities, prompt notice shall be given to recipient management officials above the level of involvement. The recipient, in turn, shall promptly notify the cognizant Federal agency of the illegal acts or irregularities and of proposed and actual actions, if any.

## **Audits of Commercial/For-Profit Organizations**

These organizations shall have financial and compliance audits conducted by qualified individuals who are organizationally, personally, and externally independent from those who authorize the expenditure of Federal funds. This audit must be performed in accordance with Government Auditing Standards, 1994 Revision. The purpose of this audit is to ascertain the effectiveness of the financial management systems and internal procedures that have been established to meet the terms and conditions of the award. Usually, these audits shall be conducted annually, but not less frequently than every two years. The dollar threshold for audit reports established in OMB Circular A-133, as amended, applies.

## **Audits of Subrecipients**

When subawards are made to another organization or organizations, the recipient shall require that subrecipients comply with the audit requirements set forth in OMB Circular A-133.

Recipients are responsible for ensuring that subrecipient audit reports are received and for resolving any audit findings. Known or suspected violations of any law encountered during audits, including fraud, theft, embezzlement, forgery, or other serious irregularities, must be communicated to the recipient and to DHS. Criminal violations must also be reported to the appropriate law enforcement agencies.

For subrecipients who are not required to have an audit as stipulated in OMB Circular A-133, the recipient is still responsible for monitoring the subrecipients' activities to provide reasonable assurance that the subrecipient administered Federal awards in compliance with Federal requirements.

## **Distribution of Reports**

The submission of audit reports for all grantees shall be as follows:

1. **State and Local Governments, Institutions of Higher Education, and Non-Profit Institutions** - All completed audit reports for State and local governments, institutions of higher education, and non-profit institutions should be mailed to the Federal Audit Clearinghouse, Bureau of the Census, 1201 East 10th Street, Jeffersonville, IN 47132.
2. **Commercial Organizations and Individuals** - One copy of all audit reports for commercial organizations and individuals should be mailed to the Department of Homeland Security, Office of Grants and Training, Office of Grant Operations, 810 7<sup>th</sup> Street NW, Washington, DC 20531.

## **Technical Assistance**

The DHS Office of the Inspector General is available to provide technical assistance to recipients in implementing the audit requirements when DHS is the assigned cognizant

agency or has oversight responsibilities because it provided the preponderance of direct Federal funding to the recipient. This assistance is available for areas such as:

1. Review of the audit arrangements and/or negotiations;
2. Review of the audit program or guide to be used for the conduct of the audit; and
3. On-site assistance in the performance of the audit, when deemed necessary, as a result of universal or complex problems that arise.

## Chapter 13: Close Out

Highlights from this chapter:

- Close Out Process
- Retention and Maintenance of Records
- Access to Records

# Close Out

## Close Out Process

Within **90 days after the end date of the award** or any approved extension thereof (revised end date), the recipient must submit the required close-out documents to G&T. Prior to submission of these documents, the recipient should do the following:

1. **Cash Reconciliation** - The recipient should request reimbursement for any funds due to cover expenditures and obligations (incurred prior to the grant expiration date and liquidated within 90 days after the grant expiration date) at award closeout. The recipient expenditures (outlays) must be equal to or greater than the cash disbursements from G&T.
2. **Drawdown of Funds** – The recipient should request final payment for reimbursement of expenditures made within the approved period in conjunction with the final financial status report.

**In order to close-out an award**, the recipient must submit the following documents to G&T:

1. **Final Financial Status Report** - This final report of expenditures must have no unliquidated obligations and must indicate the exact balance of unobligated funds. Any unobligated/unexpended funds will be deobligated from the award amount by G&T.
2. **Final Progress Report** - This report should be prepared in accordance with instructions provided by G&T.
3. **Invention or Patent Report** - All inventions that were conceived or first actually reduced to practice during the course of work under the award project must be listed on this report before closeout. (if applicable)
4. **Disposition or recovery of Federally owned assets.**
5. **Federally owned property report.**
6. Any other documents as required by the program guidance or award terms and conditions.

If funds must be returned at award closeout, award recipients should remit their check with a cover letter indicating the grant award number, the unobligated balance, and the itemization of returned monies, e.g., excess payments, interest income, program income, questioned costs, payments to vendors, etc. Award recipients should contact the Office of Grant Operations ([ASK-OGO@DHS.GOV](mailto:ASK-OGO@DHS.GOV) or 1-866-9ASK-OGO) for further instructions.

## Retention and Maintenance of Records

In accordance with the requirements set forth in the OMB administrative requirements circulars, all financial records, supporting documents, statistical records, and all other records pertinent to the award shall be retained by each organization for at least three years from the date of submission of the final expenditure report. In cases where litigation, a claim, or an audit is initiated prior to expiration of the three year period,

records must be retained until completion of the action and resolution of issues or the end of the three year period, whichever is later. Retention is required for purposes of Federal examination and audit. Records may be retained in an automated format. State or local governments may impose record retention and maintenance requirements in addition to those prescribed.

1. **Coverage** - The retention requirement extends to books of original entry, source documents supporting accounting transactions, the general ledger, subsidiary ledgers, personnel and payroll records, cancelled checks, and related documents and records. Source documents include copies of all awards, applications, and required recipient financial and narrative reports. Personnel and payroll records shall include the time and attendance reports for all individuals reimbursed under the award, whether they are employed fulltime or part-time. Time and effort reports are also required for consultants, as well as justification of consultant rates in accordance with market value.
2. **Retention Period** - The three year retention period starts from the date of submission of the final expenditure report. If any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the three year period, the records must be retained until completion of the action and resolution of all issues that arise from it or until the end of the regular three year period, whichever is later.

Recipients of funds are expected to see that records of different Federal fiscal periods are separately identified and maintained so that information desired may be readily located. Recipients are also obligated to protect records adequately against fire or other damage. When records are stored away from the recipient's principal office, a written index of the location of records stored should be on hand and ready access should be assured.

## **Access to Records**

G&T, DHS, the DHS Office of the Inspector General, the Comptroller General of the United States, or any of their authorized representatives, will have the right of access to any pertinent books, documents, papers, or other records of recipients that are pertinent to the award, in order to make audits, examinations, excerpts, and transcripts. The right of access must not be limited to the required retention period, but shall last as long as the records are retained.

However, only under extraordinary and rare circumstances would such access include review of the true name of confidential informants or victims of crime. When access to the true name of confidential informants or victims of crime is necessary, appropriate steps to protect this sensitive information must and will be taken by the recipient and G&T. Any such access, other than under a court order or subpoena pursuant to a bona fide confidential investigation, must be approved by G&T.

## **Appendix:      Glossary of Terms**

## Glossary of Terms

**Accrual Basis** is the method of recording revenues in the period in which they are earned, regardless of when cash is received, and reporting expenses in the period when the charges are incurred, regardless of when payment is made.

**Administrative Requirements** are standards for consistency and uniformity in the administration of grants, cooperative agreements, and subawards.

**Amusement/social event** is an informal gathering that is not mandatory for all participants to attain the necessary information. An indicator of a social/amusement event is a cash bar.

**Awarding agency** is the Federal government or the next highest authority, i.e., the State agency administering the formula award or the Federal agency administering the discretionary award.

**Awards** may include funding mechanisms such as grants, cooperative agreements, interagency agreements, contracts, and/or other agreements.

**Breaks** are short pauses in an ongoing informational program at trainings, meetings, conferences, or retreats. Typically, an all-day event may include one break during a morning session and one break during an afternoon session.

**Break foods** consist of cookies, sodas, and fruits or other snack items, and may be served at a training program, a meeting, or a conference.

**Budget Period** is the period for which a budget is approved for an award. The budget period may be equal to or shorter than the project period for an award, but cannot be longer than the project period.

**Cash Basis** is the method of reporting revenues and expenses when cash is actually received or paid out.

**Closeout** is a process in which G&T determines that all applicable administrative actions and all required work of the award have been completed by the recipient and G&T.

**Cognizant Federal agency** is the Federal agency that generally provides the most Federal financial assistance to the recipient of funds. Cognizance is assigned by the Office of Management and Budget (OMB). Cognizant agency assignments for the largest cities and counties are published in the Federal Register. The most recent publication was dated January 6, 1986. The cognizant agency is generally the agency that will negotiate an organization's indirect cost rate agreement. The cognizant agency is also responsible for resolution of A-133 audit findings.

**Conference or meeting** is a formal event involving topical matters of general interest (i.e., matters that will contribute to improved conduct, supervision, or management of the agency's functions or activities) to Federal agency and non-Federal agency participants, rather than a routine business meeting primarily involving day-to-day agency operations

and concerns. "Meeting" includes other designations, such as a conference, congress, convention, seminar, symposium, training for grantees or contractors, and workshop.

**Consultant** is an individual who provides professional advice or services.

**Continental breakfast** means a light breakfast that may include a selection of coffees, teas, juices, fruits, and assorted pastries, and is allowable provided several hours of substantive material directly follows the continental breakfast. Grant recipients are reminded that the least expensive of the available selections should be chosen. If a meal is provided to the recipient, per diem must be reduced accordingly.

**Contracts** are entered into by the awarding agency, recipients or subrecipients, and commercial (profit making) and non-profit organizations. With the exception of a few justified sole source situations, contracts are awarded via competitive processes to procure a good or service.

**Cooperative agreements** are awarded to States, units of local government, or private organizations at the discretion of the awarding agency or as stipulated by law. Cooperative agreements are utilized when substantial involvement is anticipated between the awarding agency and the recipient during performance of the contemplated activity.

**Discretionary awards** are made to States, units of local government, or private organizations at the discretion of the awarding agency or as stipulated by law. Most discretionary awards are competitive in nature in that there are limited funds available and a large number of potential recipients.

**Domestic travel** includes travel within and between Canada and the United States and its territories and possessions.

**Equipment** is tangible, nonexpendable, personal property having a useful life of more than one year and an acquisition cost of \$5,000 or more per unit. A recipient/subrecipient may use its own definition of equipment provided that such definition would at least include all equipment defined above.

**Federal contractor** is a person or entity that contracts with the Federal government to provide supplies, services, or experimental, developmental, or research work. Entities may include commercial organizations, educational institutions, construction and architectural engineering companies, State and local governments, and non-profit organizations.

**Federal employees** are people employed in or under an agency of the United States Federal Government.

**Federal grantee** means the component of a State, local, or Federally recognized Indian tribal government, educational institution, hospital, or a for profit or non-profit organization that is responsible for the performance or administration of all or some part of a Federal award.

**Focus group** means a gathering of Federal government employees to discuss results and improvements of programs in the field. The focus group should follow a prepared agenda, be led by an expert in the subject matter, and serve to educate Federal employees.

**Food and/or beverages** retain their common meanings. Food or beverages are considered in the context of formal meals and in the context of refreshments served at short, intermittent breaks during an activity. Beverages do not include alcoholic drinks.

**Foreign travel** includes any travel outside of Canada and the United States and its territories and possessions. For an organization located in a foreign country, this means travel outside that country.

**Formal agenda** provides a list of all activities that shall occur during the event, using an hour-by-hour time line. It must specifically include the times during the event when food and beverages will be provided.

**Formula awards** are awarded to the States to provide assistance to State and local units of government for programs in accordance with legislative requirements.

**Grants** are awarded to States, units of local government, or private organizations at the discretion of the awarding agency or on the basis of a formula. Grants are used to support a public purpose of support or stimulation authorized by Federal statute.

**High risk** is a determination made by the awarding agency of a recipient's ability to financially administer Federal project funds. Additional requirements, such as reporting and/or monitoring, may be imposed.

**Incidental** means relating to a formal event where full participation by participants mandates the provision of food and beverages.

**Indirect costs** are costs of an organization that are not readily assignable to a particular project, but are necessary to the operation of the organization and the performance of the project. The cost of operating and maintaining facilities, depreciation, and administrative salaries are examples of the types of costs that are usually treated as indirect.

**Interagency agreements** and purchase of service arrangements are usually entered into by two governmental units or agencies. Such funding arrangements are negotiated by the entities involved.

**Match** is the recipient share of the project cost. Match may either be "in-kind" or "cash." In-kind match includes the value of donated services. Cash match includes actual cash spent by the recipient and must have a cost relationship to the Federal award that is being matched.

**Nonexpendable personal property** includes tangible personal property having a useful life of more than one year and an acquisition cost of \$5,000 or more per unit. A recipient may use its own definition of nonexpendable personal property provided that the definition would at least include all tangible personal property.

**Obligation** means a legally binding liability to pay under a grant, subgrant, and/or contract determinable sums for services or goods incurred during the grant period.

**Pass-through** is an obligation on the part of the States to make funds available to units of local governments, combinations of local units, or other specified groups or organizations.

**Personal property** means property of any kind except real property. It may be tangible (having physical existence) or intangible (having no physical existence, such as patents, inventions, and copyrights).

**Preagreement/Pre-award** costs are defined as costs that are considered necessary to the project but occur prior to the starting date of the award period.

**Prior approval** means written approval by the authorized official (the next highest authority except for sole source) evidencing consent prior to a budgetary or programmatic change in the award.

**Program income** means gross income earned by the recipient during the funding period as a direct result of the award. Direct result is defined as a specific act or set of activities that are directly attributable to grant funds and that are directly related to the goals and objectives of the project. Determinations of "direct result" will be made by the awarding agency for discretionary grants and by the State for formula subawards. Fines/penalties are not considered program income. Program income may be used only for allowable program expenses.

**Project Period** is the period for which implementation of a project is authorized. The project period may be equal to or longer than the budget period for an award, but cannot be shorter than the budget period.

**Real property** means land, land improvements, structures, and appurtenances thereto, excluding movable machinery and equipment.

**Reasonable** costs are costs that a prudent person would have incurred under the circumstances prevailing at the time the decision to incur the cost was made. Costs to consider when making judgments about reasonableness include the cost of food and beverage, total cost of the event, and costs incurred relative to costs in the geographical area. The exception to this definition is lodging costs for events of 30 or more participants, when the event is funded with a G&T award. For these events, reasonable is defined as the Federal per diem rate for lodging.

**Reception** means an informal gathering that is not mandatory for all event participants to obtain necessary information. Indicators of a reception include a cash bar, inadequate seating for the entire group, food items from a reception menu (such as finger foods), and a longer break (than utilized throughout the day) between the substantive meetings and the reception. Receptions are expressly prohibited and are considered to be an unallowable cost with Federal funds.

**Recipient** is an individual and/or organization that receives Federal financial assistance directly from the Federal agency.

**Social event** is any event with alcoholic beverages served, available, or present. Social events are expressly prohibited and are considered to be an unallowable cost with Federal funds.

**Stipend** is an allowance for living expenses. Examples of these expenses include, but are not limited to, rent, utilities, incidentals, etc.

**Subaward** is an award of financial assistance in the form of money to an eligible subrecipient or a procurement contract made under an award by a recipient.

**Subrecipient** is an individual and/or organization that receives Federal financial assistance from the direct recipient of Federal funds. This may include entities receiving funds as a result of formula awards.

**Supplanting** is to deliberately reduce State or local funds because of the existence of Federal funds. For example, when State funds are appropriated for a stated purpose and Federal funds are awarded for that same purpose, the State replaces its State funds with Federal funds, thereby reducing the total amount available for the stated purpose.

**Working dinner** means a formal and mandatory dinner necessary for all participants to have full participation in the conference or event. A working dinner must include a formal agenda including a program or speakers that will impart necessary information important for full understanding of the subject matter of the conference. There should be several hours of informative sessions providing substantive information scheduled both before and after a working dinner. Indicators of a working dinner include seating for all participants. If a meal is provided to the recipient, per diem must be reduced accordingly.

**Working lunch** is a formal and mandatory lunch necessary for all participants to have full participation in the conference or event. A working lunch must include a formal agenda including a program or speakers that will impart necessary information important for full understanding of the subject matter of the conference. There should be several hours of informative sessions providing substantive information scheduled both before and after a working lunch (exhibits are not included). Indicators of a working lunch include seating for all participants. If a meal is provided to the recipient, per diem must be reduced accordingly.

**Work-related event** is a conference or meeting involving a topical matter of interest within the purview of the agency's mission and function.

# Index

# Index

Access to Records, 6, 54, 56  
Accounting Responsibilities, 5, 19, 20  
Accounting System, 13  
Accrual, 61  
Adjustments to Awards, 5, 32, 33  
Administrative Requirements, 8, 61  
Audit, 6, 9, 21, 45, 50, 51, 52  
Award Document, 5, 15, 16  
Bonding, 21  
Bonuses or Commissions, 43  
Buy American Act, 40  
Cash Management Improvement Act, 5, 24, 25  
Close Out, 6, 54, 55  
Commingling of Funds, 5, 19, 21  
Compensation of Federal Employees, 43  
Conflicts of Interest, 5, 19, 22  
Construction or Renovation, 45  
Consultant, 41, 62  
Cooperative agreements, 17, 62  
Cost Analysis, 5, 11, 14  
Direct Recipients, 9  
Drawdown, 55  
Dun & Bradstreet (D&B), 13  
DUNS, 13  
Equipment, 40, 62  
Financial Status Report, 31, 34, 36, 37, 55  
Fly America Act, 46  
Foreign Travel, 46  
Fund Raising, 44  
Grants, 1, 3, 4, 8, 12, 17, 26, 31, 34, 52, 58, 63  
Indirect Costs, 41  
Individuals, 10, 13, 52  
Interest, 5, 24, 26, 36, 45  
Lobbying, 44  
Management and Administrative, 41, 42  
Match, 12, 35, 37, 38, 63  
Monitoring, 5, 19, 21, 22  
Obligation of Funds, 5, 27, 28  
OMB Circulars, 8, 9, 10, 17, 21, 37, 40, 44, 45, 48, 51, 52, 61  
Payments, 5, 24, 25  
Preagreement Costs, 45  
Procurement, 6, 47, 48  
Program Income, 6, 35, 36, 37  
Reporting requirements, 31  
Retention and Maintenance of Records, 6, 54, 55  
Sole Source, 6, 48  
Special Conditions, 8, 16, 25, 34  
Subrecipients, 4, 6, 9, 10, 17, 20, 21, 22, 25, 26, 34, 37, 38, 41, 44, 45, 48, 49, 50, 51, 52, 62  
Supplanting, 5, 19, 23, 65  
Suspension, 5, 27, 28  
Termination, 5, 27, 28  
Waiver of Match Requirement, 38



**Subaward Agreement Regarding FY 2020 State Homeland Security Grant Programs**  
**Funding for Equipment, Planning, Administration, Training and Exercises**

**THIS AGREEMENT** is entered into by and between the County of Tulare ("COUNTY") and City of Visalia ("SUBRECIPIENT"), referred to individually herein as "Party" or collectively as "Parties," on the following terms and conditions:

WHEREAS, the Fiscal Year 2020 ("FY 2020") California State Homeland Security Grant Program ("SHSGP") provides funding through Federal grants from the Department of Homeland Security to enhance the capabilities of state and local first responders by allowing the purchase of advanced types of equipment, as well as addressing other critical homeland security needs, including administration, planning, training, and exercise-related costs;

WHEREAS, COUNTY applied to the California Governor's Office of Emergency Services ("CalOES") for a FY 2020 SHSGP grant;

WHEREAS, as part of its grant application, COUNTY requested sufficient funds to support certain activity(ies) or program(s) planned by SUBRECIPIENT that may be eligible for SHSGP grant funds;

WHEREAS, COUNTY was awarded FY 2020 SHSGP grant funding; and COUNTY, upon recommendation of the local Approval Authority designated in the SHSGP Guidelines, determined to allocate some of this funding to support SUBRECIPIENT'S eligible program(s) or activity(ies).

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and intending to be legally bound hereby, COUNTY and SUBRECIPIENT hereby agree as follows:

**1. GRANT SUBAWARD.** Subject to the terms, conditions, and other limitations specified herein, COUNTY intends to subaward to SUBRECIPIENT a portion of its FY 2020 SHSGP Grant for the following program and/or activity:

**Department/Agency:** City of Visalia

---

**Program/Activity:** (1) Hazmat Technician/ Specialist Class Series Tuition \$34,000 and Travel \$22,907,

---

(1) Hazmat Technician/ Specialist Class Series Tuition \$19,500 and Travel \$11,453

---

Details about the specific program or activity authorized, the amounts allocated to the specified program or activity, and the anticipated performance and disbursement timelines shall be confirmed by subsequent award letter(s) from COUNTY ("Award Letter(s)") in accordance with this Agreement. **SUBRECIPIENT agrees not to expend any anticipated FY 2020 SHSGP grant funds until after it has received [an] Award Letter(s) authorizing the specific activity or program, and confirming the award amount.** Award Letter(s) may include attachments, which are considered to be integral parts of the Award Letter(s). Unless SUBRECIPIENT notifies COUNTY before it begins spending the funds authorized in a FY 20120 SHSGP Award Letter that it declines some or all of the program, activity, and/or funds outlined in the Award Letter, SUBRECIPIENT will be deemed to have accepted all of the terms and conditions specified in the Award Letter(s), including any applicable attachments.

COUNTY reserves the exclusive right to determine the method and timing of disbursement of SHSGP funds to SUBRECIPIENT. Furthermore, and in addition to all other rights provided to COUNTY under

this Agreement or the law, COUNTY reserves the right to, issue revised Award Letter(s) to modify SUBRECIPIENT's authorized program, activity, award amounts, and/or performance periods, in accordance with the recommendations of the Local Approval Authority, the changing needs of SUBRECIPIENT and/or the likelihood of SUBRECIPIENT expending its subaward; however, such modifications will only be made after consultation with SUBRECIPIENT, and in accordance with the recommendations of the Local Approval Authority.

**2. PERFORMANCE PERIOD.** SUBRECIPIENT's Performance Period for all activities covered by the terms of this Agreement shall commence on October 1, 20120. Unless COUNTY specifies otherwise in SUBRECIPIENT's Award Letter(s), SUBRECIPIENT's Performance Period for all activities covered by the terms of this Agreement shall continue until whichever of the following dates or events occurs first: (i) April 30, 2022, or (ii) until otherwise terminated under the provisions of this Agreement. Only activities performed during the County-specified FY 2020 SHSGP Performance Period are eligible for funding/reimbursement pursuant to this Agreement.

**3. GRANT REQUIREMENTS AND ASSURANCES.** The SUBRECIPIENT hereby agrees to review, adhere to, and comply with all COUNTY, state, and federal grant award requirements. SUBRECIPIENT acknowledges that COUNTY was required to accept and agree to the "**CalOES Standard Assurances**" (attached as **Exhibit A**, and incorporated by reference herein), and that COUNTY may be required to impose some or all of these assurances on all of its subrecipients, at all levels. Accordingly, SUBRECIPIENT specifically accepts, agrees to, and will abide by the CalOES Standard Assurances, with the understanding that everywhere it references "Applicant" or "subrecipient" in Exhibit A shall be read to refer to SUBRECIPIENT. The CalOES Standard Assurances shall be binding on the SUBRECIPIENT, as well as its successors, transferees, contractors, consultants, etc. SUBRECIPIENT acknowledges that failure to comply with any of the assurances may result in suspension, termination, or reduction of grant funds.

Some of the requirements that SUBRECIPIENT hereby agrees to comply with appear in the following documents:

- (a) Applicable Federal Regulations, including: (i) Title 2, Part 200 of the Code of Federal Regulations (CFR) (which contains, among other items, Government cost principles, uniform administrative requirements and audit requirements for Federal grant programs), and (ii) updates issued by the Office of Management and Budget (OMB) on <http://www.whitehouse.gov/omb/>;
- (b) Federal Program Notice of Funding Opportunity (NOFO);
- (c) California Supplement to the NOFO; and
- (d) Federal and State Grant Program Guidelines.

By signing this Agreement, SUBRECIPIENT specifically makes the applicable certifications in Exhibit A, including the Lobbying and Political Activities and Debarment and Suspension Certifications (Paragraphs 3 and 4 of Exhibit A, respectively), as evidenced by the signature of SUBRECIPIENT's authorized agent.

**4. FEDERALLY-FUNDED SERVICES.** Because this grant subaward involves the provision of federal funds to SUBRECIPIENT, the terms and conditions outlined and incorporated in **Exhibit B, "Federally-Funded Services,"** will apply to this Agreement, and are incorporated herein by reference.

**5. DISPOSAL OR DISPOSITION OF PROPERTY.** SUBRECIPIENT acknowledges that pursuant to 2 CFR section 200.316, any real property, equipment, and intangible property that are acquired or improved

with any SHSGP award must be held in trust by SUBRECIPIENT as trustee for the beneficiaries of the project or program under which the property was acquired or improved. SUBRECIPIENT may be required by COUNTY, CalOES, or the federal government to record liens or other appropriate notices of record to indicate that personal or real property has been acquired or improved with the SHSGP award and that use and disposition conditions apply to the property.

Furthermore, SUBRECIPIENT agrees that when the equipment or supplies acquired with funds from this subaward are no longer needed for the original activity or program, or for other SUBRECIPIENT activities supported by the Department of Homeland Security (DHS)/ Federal Emergency Management Agency (FEMA), SUBRECIPIENT must notify COUNTY to request instructions on proper disposition of the equipment or supplies. SUBRECIPIENT is not permitted to sell, assign, or otherwise transfer title to (or any other interest in) equipment or supplies purchased with SHSGP funds except as permitted by 2 CFR Part 200. Furthermore, SUBRECIPIENT must obtain the express written permission of COUNTY for disposition of property that may have a current per unit fair market value of \$5,000 or more. Though not exclusive or exhaustive, additional information regarding disposition of property acquired with SHSGP funds can be found at 2 CFR Part 200, sections 200.313 through 200.316.

**6. SUBAWARDS AND CONTRACTS.** With the understanding that not all provisions may be applicable to subawardees, SUBRECIPIENT agrees to include all of the commitments specified in Exhibit A, and any other commitments or requirements included in this Agreement that expressly so designate, in the award documents it issues for all subawards at all tiers, including contracts under grants and cooperative agreements and subcontracts. SUBRECIPIENT further agrees that it will include the commitments in Exhibit A in all contracts paid for in full or part with FY 2020 SGHSGP funds.

**7. DESIGNATED COUNTY AUTHORIZED AGENT.** Only those individuals designated by resolution of the Tulare County Board of Supervisors as Authorized Agents for FY 2020 SHSGP ("COUNTY Authorized Agents") are authorized to sign FY 2020 SHSGP Award Letters on behalf of COUNTY, or to suspend performance in accordance with Paragraph 16(d), below. All other notices from COUNTY may come from other COUNTY personnel.

**8. PROOF OF SUBRECIPIENT AUTHORITY.** Before this Agreement will be approved by COUNTY, SUBRECIPIENT must provide to COUNTY written authorization (in the form of a resolution, or some other format specifically authorized by COUNTY) from the city council, governing board, or authorized body in support of this project. This written authorization must specify that the SUBRECIPIENT and the city council, governing board, or authorized body agree:

- (a) To provide all matching funds required for the grant project and that any cash match will be appropriated as required;
- (b) Any liability arising out of performance of this Agreement shall be the responsibility of the SUBRECIPIENT and the city council, governing board, or authorized body;
- (c) Grant funds shall not be used to supplant expenditures controlled by the city council, governing board, or authorized body;
- (d) SUBRECIPIENT is authorized by the city council, governing board, or authorized body to apply for federal assistance, and the institutional, managerial, and financial capability (including funds sufficient to pay the non-federal share of project cost, if any) to ensure proper planning, management, and completion of the project described in this application; and
- (e) Official executing this Agreement is authorized by the SUBRECIPIENT.

**9. DISALLOWANCE AND OFFSET.** If, pursuant to this Agreement, SUBRECIPIENT requests or receives payment from COUNTY for programs, activities, or equipment, the reimbursement for which is later disallowed by the State of California or the United States Government, SUBRECIPIENT shall promptly refund the disallowed amount to COUNTY upon COUNTY's request. At its option, and to the fullest extent permitted by law, COUNTY may offset the amount disallowed from any payment due or to become due to SUBRECIPIENT under this Agreement or any other agreement between SUBRECIPIENT or COUNTY.

Furthermore, if any of COUNTY's FY 20120 SHSGP grant funding is reduced, modified, or eliminated for any reason, COUNTY reserves the right to reduce, modify, or eliminate any or all of this FY 2020 SHSGP grant subaward to SUBRECIPIENT. SUBRECIPIENT agrees to promptly return any amounts requested by COUNTY in accordance with this provision. At its option, COUNTY may offset the amount to be returned by SUBRECIPIENT from any payment due or to become due to SUBRECIPIENT under this Agreement or any other agreement between SUBRECIPIENT and COUNTY.

**10. MONITORING AND REPORTS.** SUBRECIPIENT is responsible for oversight of the operations of the FY 2020 SHSGP supported activities. SUBRECIPIENT must monitor its activities to ensure compliance with applicable Federal requirements and achievement of specific performance expectations. SUBRECIPIENT's monitoring must cover each program, function or activity supported by FY 2020 SHSGP funding.

SUBRECIPIENT agrees to provide ongoing performance and financial reports regarding any and all of SUBRECIPIENT's programs and activities funded with FY 2020 SHSGP funding. At a minimum, these reports will be due on an annual basis, but COUNTY reserves the right to request more frequent reporting. Within 90 days of completion or termination of FY 2020 SHSGP funded subawards, SUBRECIPIENT is also expected to provide a final performance report and a final expenditure report in a format acceptable to COUNTY, State and the Federal government. SUBRECIPIENT will be notified of any additional required reports by separate Award Letter(s) or notice(s) from COUNTY.

**11. MANDATORY DISCLOSURES.** Pursuant to 2 CFR section 200.113, SUBRECIPIENT must disclose, in a timely manner, and in writing to COUNTY and ultimately to the federal awarding agency, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting this subaward. Pursuant to the terms and conditions outlined in Appendix XII to 2 CFR Part 200 ("Award Term and Condition for Recipient Integrity and Performance Matters"), SUBRECIPIENT may also be required to report certain civil, criminal, or administrative proceedings to SAM. Failure to make required disclosures can result in any of the remedies described in 2 CFR section 200.338, "Remedies for noncompliance," including suspension or debarment.

**12. SUBMITTING FALSE CLAIMS.** Under applicable federal and state law, if SUBRECIPIENT submits a false claim to COUNTY under this Agreement, then SUBRECIPIENT will be liable to COUNTY for the statutory penalties set forth in those statutes, including, but not limited to statutory fines, treble damages, costs, and attorneys' fees. SUBRECIPIENT will be deemed to have submitted a false claim to COUNTY if SUBRECIPIENT:

- (a) Knowingly presents or causes to be presented to COUNTY a false claim or request for payment or approval;
- (b) Knowingly makes, uses, or causes to be made or used a false record or statement to get a false claim paid or approved by COUNTY;
- (c) Conspires to defraud COUNTY, State, or the Federal Government by getting a false claim

allowed or paid by COUNTY

- (d) Knowingly makes, uses, or causes to be made or used a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to COUNTY; or
- (e) Is a beneficiary of an inadvertent submission of a false claim to COUNTY, later discovers the falsity of the claim, and fails to disclose the false claim to COUNTY within a reasonable time after discovery of the false claim.

**13. INSURANCE.** SUBRECIPIENT certifies it is insured or self-insured for general liability exposures with limits of no less than \$1 million per occurrence. SUBRECIPIENT certifies it is insured or self-insured for workers' compensation and maintains statutory limits. SUBRECIPIENT agrees that coverage limits specified within the Agreement will not be used to reduce limits of coverage from SUBRECIPIENT'S full policy limits. Insurance Policies will not be used to limit liability or to limit the indemnification provisions and requirements of this Agreement or act in any way to reduce available coverage and limits from the insurer. Failure to maintain or renew coverage may be a material breach of this Agreement.

**14. LIABILITY OF COUNTY.** COUNTY's payment obligations to SUBRECIPIENT for FY 2020 SHSGP funds are limited by all provisions and other requirements specified in this Agreement. Notwithstanding any other provision of this Agreement, in no event shall COUNTY be liable, regardless of whether any claim is based on contract or tort, for any special, consequential, indirect, or incidental damages arising out of or in connection with this Agreement, including, but not limited to, lost profits, equipment purchased, or activities performed in connection with this Agreement.

**15. HOLD HARMLESS, INDEMNIFICATION, AND DEFENSE.**

(a) To the fullest extent permitted by law, SUBRECIPIENT must indemnify, defend (at SUBRECIPIENT'S sole cost and expense and with legal counsel approved by COUNTY, which approval may not be unreasonably withheld), protect, and hold harmless COUNTY, all subsidiaries, divisions and affiliated agencies of COUNTY, and all of their representatives, partners, designees, officers, directors, employees, consultants, agents, successors and assigns, (each, an "Indemnified Party" and collectively, the "Indemnified Parties"), from and against all claims (including, without limitation, claims for bodily injury, death or damage to property), demands, obligations, damages, actions, causes of action, suits, losses, judgments, fines, penalties, liabilities, costs and expenses (including, without limitation, attorneys' fees, disbursements and court costs, and all other professional expert or consultants' fees and costs and COUNTY general and administrative expenses) of every kind and nature whatsoever (individually, a "Claim"; collectively, "Claims") which may arise out of, pertain to, or relate (directly or indirectly) to the negligence, recklessness, or misconduct of SUBRECIPIENT with respect to any activities and/or programs performed, training provided, or items purchased or used under or in relation to this Agreement (including, without limitation, the acts, errors, and/or omissions of SUBRECIPIENT, its principals, officers, agents, employees, vendors, suppliers, consultants, sub-consultants, contractors, anyone employed directly or indirectly by any of them, or for whose acts they may be liable, or any or all of them). SUBRECIPIENT'S obligation to indemnify applies unless it is finally adjudicated that the liability was caused by the sole active negligence or sole willful misconduct of an Indemnified Party. If it is finally adjudicated that liability is caused by the comparative active negligence or willful misconduct of an Indemnified Party, then SUBRECIPIENT'S indemnification obligation shall be reduced in proportion to the established comparative liability.

(b) The duty to defend is a separate and distinct obligation from SUBRECIPIENT'S duty to indemnify. SUBRECIPIENT shall be obligated to defend, in all legal, equitable, administrative, or special proceedings, the Indemnified Parties immediately upon tender to SUBRECIPIENT of the Claim in any form

or at any stage of an action or proceeding, whether or not liability is established. Payment to SUBRECIPIENT by any Indemnified Party or the payment or advance of defense costs by any Indemnified Party cannot be a condition precedent to enforcing the Indemnified Party's rights to defense or indemnification under this Agreement. An allegation or determination that persons other than SUBRECIPIENT are responsible for the Claim does not relieve SUBRECIPIENT from its separate and distinct obligation to defend under this section. The obligation to defend extends through final judgment, including exhaustion of any appeals. The defense obligation includes an obligation to provide independent defense counsel if SUBRECIPIENT asserts that liability is caused in whole or in part by the negligence or willful misconduct of an Indemnified Party. If it is finally adjudicated that liability was caused by the comparative active negligence or willful misconduct of an Indemnified Party, then SUBRECIPIENT may submit a claim to the COUNTY for reimbursement of reasonable attorneys' fees and defense costs in proportion to the established comparative liability of the Indemnified Party. SUBRECIPIENT'S indemnification obligations under this Agreement will survive the expiration or earlier termination of this Agreement until action against the Indemnified Parties for the matter indemnified is fully and finally barred by the applicable statute of limitations or statute of repose. SUBRECIPIENT'S liability for indemnification under this Agreement is in addition to any liability SUBRECIPIENT may have to COUNTY for a breach by SUBRECIPIENT of any of the provisions of this Agreement. Under no circumstances may the insurance requirements and limits set forth in this Agreement be construed to limit SUBRECIPIENT'S indemnification obligation or other liability under this Agreement. The terms of this Agreement are contractual and the result of negotiation between the Parties.

(c) SUBRECIPIENT must indemnify and hold COUNTY harmless from all loss and liability, including attorneys' fees, court costs and all other litigation expenses, for any infringement of the patent rights, copyright, trade secret or any other proprietary right or trademark, and all other intellectual property claims of any person or persons in consequence of the use by COUNTY, or any of its officers or agents, of articles or services to be supplied in the performance of this Agreement.

## **16. TERMINATION**

(a) Without Cause (For Convenience): Either Party may terminate this Agreement for convenience by giving thirty (30) days' prior written notice to the other Party of its intention to terminate pursuant to this provision, specifying the date of termination. COUNTY will not pay lost anticipated profits or other economic loss resulting from termination of this Agreement. After receiving a notice of termination for convenience from SUBRECIPIENT, and prior to the effective date of termination, COUNTY may, in its sole discretion, continue to disburse grant funding to SUBRECIPIENT for the programs or activities permitted under this Agreement and specified in the effective Award Letter(s); however, COUNTY specifically reserves the right to cancel or modify some of the programs or activities specified in the Award Letter if it seems infeasible for SUBRECIPIENT to complete its work before the termination of the contract. Any funding disbursed to SUBRECIPIENT but not yet spent at the time the Agreement is terminated must be returned to COUNTY. All such disbursements continue to be subject to the restrictions otherwise provided in this Agreement or by law.

COUNTY will not impose sanctions on SUBRECIPIENT for a termination for convenience.

(b) With Cause: Either party may terminate this Agreement immediately, by written notice to the other Party, should the other Party:

- (1) be adjudged a bankrupt, or
- (2) become insolvent or have a receiver appointed, or
- (3) make a general assignment for the benefit of creditors, or

(4) suffer any judgment which remains unsatisfied for 30 days, and which would substantively impair the ability of the judgment debtor to perform under this Agreement.

COUNTY also reserves the right to immediately suspend and/or to terminate this Agreement, for cause, upon discovery of a material breach by SUBRECIPIENT. A material breach includes, but is not limited to, (i) SUBRECIPIENT's failure to comply with the terms and conditions of this Agreement or of any Award Letter(s) issued by COUNTY; (ii) a material misrepresentation by SUBRECIPIENT to COUNTY in relation to this grant program; or (iii) failure to comply with all applicable laws or regulations. COUNTY will provide written notice of the material breach and its determination to either suspend or terminate the contract, specifying the date of termination. At COUNTY's sole discretion, COUNTY may provide SUBRECIPIENT with a reasonable period of time to cure the breach. If COUNTY terminates this Agreement for cause, COUNTY reserves the right to reduce, modify, or eliminate any or all of this subaward and any other outstanding SHSGP subawards to SUBRECIPIENT. Upon demand by COUNTY, SUBRECIPIENT agrees to immediately return FY 2020 SHSGP funding that has been disbursed to SUBRECIPIENT and which remains in SUBRECIPIENT's possession at the time this Agreement is terminated. In addition, the payment of any grant funds that have yet to be disbursed for work already completed by SUBRECIPIENT under this Agreement remains subject to the restrictions on payments otherwise provided in this Agreement and by law, and is further conditioned on COUNTY's confirmation of SUBRECIPIENT's satisfactory completion of the activities or programs specified in this Agreement and any related Award Letter(s).

COUNTY will not pay lost anticipated profits or other economic loss, nor will the County pay compensation or make reimbursement to cure any breach arising out of or resulting from such termination for cause. If this Agreement is terminated for cause, COUNTY may impose sanctions, including possible rejection of future proposals based on specific causes of non-performance. Furthermore, if this Agreement is terminated for SUBRECIPIENT's failure to comply with applicable federal statutes or regulations, including those specifically incorporated into this Agreement by reference, SUBRECIPIENT is advised that the COUNTY's termination decision may be considered in evaluating future applications for federal grant awards.

(c) Effects of Completion or Termination: Expiration, completion, or termination of this Agreement shall not terminate any of SUBRECIPIENT's obligations to indemnify, defend, or hold harmless; to maintain and make available any records pertaining to the Agreement; to cooperate with any audit; to be subject to offset; to make any reports of pre-termination contract activities; to honor its obligations related to the disposal or disposition of property purchased with SHSGP funding; to comply with the continuing applicable obligations contained in Exhibit A; or to comply with any other continuing or closeout obligations required by this Agreement or by federal or state law or regulation, including those specified in 2 CFR Part 200. Where SUBRECIPIENT's activities or programs have been terminated by the COUNTY for cause, said termination will not affect any rights of the COUNTY to recover damages from or against SUBRECIPIENT.

(d) Suspension of Performance: Independent of any right to terminate this Agreement, COUNTY Authorized Agents may immediately suspend performance by SUBRECIPIENT, in whole or in part, in response to health, safety or financial emergency, a change in SHSGP grant funding to COUNTY, or a failure or refusal by SUBRECIPIENT to comply with the provisions of this Agreement, until such time as the cause for suspension is resolved, or a notice of termination becomes effective.

**17. RECORDS.** SUBRECIPIENT shall maintain complete and accurate records with respect to the activities, programs, and/or purchases funded by or related to FY 20120 SHSGP funding and/or this Agreement, including all records relating to procurement of goods and services. In addition,

SUBRECIPIENT shall maintain complete and accurate records with respect to any payments to employees, subawardees, contractors, or subcontractors. All such records shall be prepared in accordance with generally accepted accounting procedures and any applicable procedures required by the COUNTY or the federal or state government. All applicable records shall be clearly identified, maintained on site, and be kept readily accessible.

SUBRECIPIENT further agrees to make all such records available to federal, state, and COUNTY government representatives, as further specified in Exhibit A, Paragraph 9 and Exhibit B, Paragraph 10. SUBRECIPIENT shall ensure that members of the public also have access to such records upon request, in accordance with the Freedom of Information Act and the California Public Records Act. SUBRECIPIENT specifically agrees to require any subrecipients, contractors, successors, transferees, and assignees to acknowledge and agree to comply with all of these record keeping and access requirements.

Failure to comply with these requirements may result in suspension of payments under the grant, termination of the grant, or both. SUBRECIPIENT may be ineligible for award of any future grants if COUNTY or Cal OES determines that any of the following has occurred: (1) the recipient has made false certification, or (2) violates the certification by failing to carry out the requirements as noted above.

**18. NOTICES.** Except as may be otherwise required by law, any notice to be given must be written and must be either personally delivered, sent by facsimile transmission, or sent by first class mail, postage prepaid and addressed as follows:

**COUNTY:**

Andrew Lockman  
Emergency Services Manager  
Tulare County HHSA/Office of Emergency Services  
5957 S Mooney Blvd  
Visalia, CA 93277  
Phone No.: (559) 624-7498  
Fax No.: (559) 624-7499

**With a Copy To:**

COUNTY ADMINISTRATIVE OFFICER  
2800 W. Burrel Ave.  
Visalia, CA 93291  
Phone No.: (559) 636-5005  
Fax No.: (559) 733-6318

**SUBRECIPIENT:**

Dan Griswold  
Fire Chief  
420 N. Burke St  
Visalia, CA 93292  
Phone No.: (559) 713-4266  
Fax No.: (559) 713-4808

Notice personally delivered is effective when delivered. Notice sent by facsimile transmission is deemed to be received upon successful transmission. Notice sent by first class mail shall be deemed received on the fifth (5<sup>th</sup>) day after the date of mailing. Either party may change the above address by giving written notice pursuant to this paragraph.

**19. CONFLICTS WITH LAWS OR REGULATIONS/ SEVERABILITY.** This Agreement is subject to all applicable laws and regulations. If any provision of this Agreement is found by any court or other legal authority, or is agreed by the parties, to be in conflict with any code or regulation governing its subject,

the conflicting provision shall be considered null and void. If the effect of nullifying any conflicting provision is such that a material benefit of the Agreement to either party is lost, the Agreement may be terminated at the option of the affected party, and some or all of the grant money may need to be returned to COUNTY. Such a termination will be treated as a termination for cause, in accordance with Paragraph 16 above. In all other cases, the remainder of the Agreement shall continue in full force and effect.

**20. MODIFICATION.** No part of this Agreement may be modified without the written consent of both Parties.

**21. EXHIBITS AND RECITALS.** The Recitals and the Exhibits to this Agreement are fully incorporated into and are integral parts of this Agreement.

**22. GOVERNING LAW.** This Agreement shall be interpreted and governed under the laws of the State of California without reference to California conflicts of law principles. The Parties agree that this contract is made in and shall be performed in Tulare County, California.

**23. FURTHER ASSURANCES.** Each Party will execute any additional documents and perform any further acts which may be reasonably required to effect the purposes of this Agreement.

**24. NO THIRD PARTY BENEFICIARIES.** Unless specifically set forth, the Parties to this Agreement do not intend to provide any other party with any benefit or enforceable legal or equitable right or remedy.

**25. WAIVERS.** The failure of either Party to insist on strict compliance with any provision of this Agreement shall not be considered a waiver of any right to do so, whether for that breach or any subsequent breach. The acceptance by either Party of either performance or payment shall not be considered to be a waiver of any preceding breach of the Agreement by the other Party.

**26. HEADINGS.** Section headings are provided for organizational purposes only and do not in any manner affect the scope, meaning or intent of the provisions under the headings.

**27. ORDER OF PRECEDENCE.** In the event of any conflict or inconsistency between or among the body of the Agreement and any Award Letter or other communication between COUNTY and SUBRECIPIENT, then the terms and conditions of the body of this Agreement shall prevail.

**28. ASSIGNMENT.** This Agreement is entered into by COUNTY in reliance on the identity and representations made by SUBRECIPIENT, and no part of this Agreement or this subaward (including any equipment purchased with the subaward) may be assigned, transferred, or sold by SUBRECIPIENT without the prior written consent of COUNTY, which consent COUNTY may grant, delay, deny, or condition in its absolute discretion. Any FY 2020 SHSGP funds provided to SUBRECIPIENT and not yet expended at the time of any attempted unauthorized assignment or transfer will be forfeit to COUNTY at the time of attempted assignment or transfer. Furthermore, the voluntary or involuntary assignment of this Agreement to a receiver or trustee in bankruptcy, will constitute a material breach and will automatically terminate this Agreement without advance notice or opportunity to cure.

**29. COMPLIANCE WITH LAWS.** SUBRECIPIENT shall comply with all applicable laws, ordinances, rules, and regulations and obtain and keep current all permits, licenses and/or approvals required by law

to perform the activities or services, or to purchase any equipment, specified in this Agreement.

**30. CONFLICT OF INTEREST**

(a) SUBRECIPIENT agrees to, at all times during the performance of this Agreement, comply with the law of the State of California regarding conflicts of interests and appearance of conflicts of interests, including, but not limited to Government Code Section 1090 et seq., and the Political Reform Act, Government Code Section 81000 et seq. and regulations promulgated pursuant thereto by the California Fair Political Practices Commission. The statutes, regulations and laws previously referenced include, but are not limited to, prohibitions against any public officer or employee, including SUBRECIPIENT, from making any decision on behalf of COUNTY in which such officer, employee or consultant/contractor has a direct or indirect financial interest. A violation can occur if the public officer, employee or consultant/contractor participates in or influences any COUNTY decision which has the potential to confer any pecuniary benefit on SUBRECIPIENT or any business firm in which SUBRECIPIENT has an interest, with certain narrow exceptions.

(b) SUBRECIPIENT agrees that if any facts come to its attention which raise any questions as to the applicability of conflicts of interest laws, it will immediately inform the COUNTY designated representative and provide all information needed for resolution of this question.

**31. COUNTERPARTS.** The Parties may sign this Agreement in counterparts, each of which is an original and all of which taken together form one single document.

**32. CERTIFICATION AND ACKNOWLEDGEMENT:** The undersigned represents that he/she is authorized to enter into this Agreement for and on behalf of the SUBRECIPIENT. As the duly authorized representative of the SUBRECIPIENT, the undersigned hereby certifies that the SUBRECIPIENT has the legal authority to apply for County, State, and Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay any non-Federal share of project cost) to ensure proper planning, management and completion of the project described in the FY 2019 SHSGP application, within the prescribed timelines.

The undersigned further acknowledges that the SUBRECIPIENT is responsible for reviewing and adhering to all COUNTY, state, and federal grant award requirements.

**[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]**

**IN WITNESS WHEREOF**, the Parties have executed this Agreement as of the day and year signed by the last Party below.

**CITY OF VISALIA**

By: \_\_\_\_\_  
Mayor

Date: \_\_\_\_\_

ATTEST:

By: \_\_\_\_\_

Approved as to form:

By: \_\_\_\_\_

**COUNTY OF TULARE**

By: \_\_\_\_\_  
Chairman, Board of Supervisors

Date: \_\_\_\_\_

ATTEST: JASON T. BRITT  
County Administrative Officer/  
Clerk of the Board of Supervisors

By: \_\_\_\_\_  
Deputy

Approved as to form: County Counsel

By: \_\_\_\_\_  
Deputy, Matter No. 20191550.

## **EXHIBIT A**



### **Standard Assurances For All Cal OES Federal Grant Programs**

**As the duly authorized representative of the Applicant, I hereby certify** that the Applicant has the legal authority to apply for federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay any non-federal share of project cost) to ensure proper planning, management, and completion of the project described in this application, within prescribed timelines.

**I further acknowledge that the Applicant is responsible for reviewing and adhering to all requirements within the:**

- (a) Applicable Federal Regulations (see below);
- (b) Federal Program Notice of Funding Opportunity (NOFO);
- (c) California Supplement to the NOFO; and
- (d) Federal and State Grant Program Guidelines.

#### **Federal Regulations**

Government cost principles, uniform administrative requirements, and audit requirements for federal grant programs are set forth in Title 2, Part 200 of the Code of Federal Regulations (C.F.R.). Updates are issued by the Office of Management and Budget (OMB) and can be found at <http://www.whitehouse.gov/omb/>.

**Significant state and federal grant award requirements (some of which appear in the documents listed above) are set forth below. The Applicant hereby agrees to comply with the following:**

#### **1. Proof of Authority**

The Applicant will obtain written authorization from the city council, governing board, or authorized body in support of this project. This written authorization must specify that the Applicant and the city council, governing board, or authorized body agree:

- (a) To provide all matching funds required for the grant project and that any cash match will be appropriated as required;
- (b) Any liability arising out of the performance of this agreement shall be the responsibility of the Applicant and the city council, governing board, or authorized body;
- (c) Grant funds shall not be used to supplant expenditures controlled by the city council, governing board, or authorized body, and
- (d) The official executing this agreement is, in fact, authorized to do so.

This Proof of Authority must be maintained on file and readily available upon request.

## **EXHIBIT A**

### **2. Period of Performance**

The Applicant will initiate work after approval of the award and complete all work within the period of performance specified in the grant.

### **3. Lobbying and Political Activities**

As required by Section 1352, Title 31 of the United States Code (U.S.C.), for persons entering into a contract, grant, loan, or cooperative agreement from an agency or requests or receives from an agency a commitment providing for the United States to insure or guarantee a loan, the Applicant certifies that:

- (a) No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
- (b) If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying", in accordance with its instructions.
- (c) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

The Applicant will also comply with provisions of the Hatch Act (5 U.S.C. §§ 1501-1508 and §§ 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds.

Finally, the Applicant agrees that federal funds will not be used, directly or indirectly, to support the enactment, repeal, modification or adoption of any law, regulation or policy without the express written approval from the California Governor's Office of Emergency Services (Cal OES) or the federal awarding agency.

### **4. Debarment and Suspension**

As required by Executive Orders 12549 and 12689, and 2 C.F.R. § 200.213 and codified in 2 C.F.R. Part 180, Debarment and Suspension, the Applicant will provide protection against waste, fraud, and abuse by debarring or suspending those persons deemed irresponsible in their dealings with the federal government. The Applicant certifies that it and its principals, subgrantees, recipients or subrecipients:

## **EXHIBIT A**

- (a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;
- (b) Have not within a three-year period preceding this application been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
- (c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in paragraph (2)(b) of this certification; and
- (d) Have not within a three-year period preceding this application had one or more public transaction (federal, state, or local) terminated for cause or default.

Where the Applicant is unable to certify to any of the statements in this certification, he or she shall attach an explanation to this application.

### **5. Non-Discrimination and Equal Employment Opportunity**

The Applicant will comply with all federal statutes relating to non-discrimination. These include, but are not limited to, the following:

- (a) Title VI of the Civil Rights Act of 1964 (Public Law (P.L.) 88-352 and 42 U.S.C. § 2000d et. seq.) which prohibits discrimination on the basis of race, color, or national origin and requires that recipients of federal financial assistance take reasonable steps to provide meaningful access to persons with limited English proficiency (LEP) to their programs and services;
- (b) Title IX of the Education Amendments of 1972, (20 U.S.C. §§ 1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex in any federally funded educational program or activity;
- (c) Section 504 of the Rehabilitation Act of 1973, (29 U.S.C. § 794), which prohibits discrimination against those with disabilities or access and functional needs;
- (d) Americans with Disabilities Act (ADA) of 1990, which prohibits discrimination on the basis of disability and requires buildings and structures be accessible to those with disabilities and access and functional needs (42 U.S.C. §§ 12101-12213);
- (e) Age Discrimination Act of 1975, (42 U.S.C. §§ 6101-6107), which prohibits discrimination on the basis of age;
- (f) Public Health Service Act of 1912 (42 U.S.C. §§ 290 dd—2), relating to confidentiality of patient records regarding substance abuse treatment;
- (g) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. § 3601 et seq.), relating to nondiscrimination in the sale, rental or financing of housing as implemented by the Department of Housing and Urban Development at 24 C.F.R. Part 100. The prohibition on disability discrimination includes the requirement that new multifamily housing with four or more dwelling units—i.e., the public and common use areas and individual apartment units (all units in buildings with elevators and ground-floor units in buildings without elevators)— be designed and constructed with certain accessible features (See 24 C.F.R. § 100.201);

## **EXHIBIT A**

- (h) Executive Order 11246, which prohibits federal contractors and federally assisted construction contractors and subcontractors, who do over \$10,000 in Government business in one year from discriminating in employment decisions on the basis of race, color, religion, sex, sexual orientation, gender identification or national origin;
- (i) Executive Order 11375, which bans discrimination on the basis of race, color, religion, sex, sexual orientation, gender identification, or national origin in hiring and employment in both the United States federal workforce and on the part of government contractors;
- (j) California Public Contract Code § 10295.3, which prohibits discrimination based on domestic partnerships and those in same sex marriages;
- (k) DHS policy to ensure the equal treatment of faith-based organizations, under which all applicants and recipients must comply with equal treatment policies and requirements contained in 6 C.F.R. Part 19;
- (l) Any other nondiscrimination provisions in the specific statute(s) under which application for federal assistance is being made; and
- (m) The requirements of any other nondiscrimination statute(s) which may apply to the application.

In addition to the items listed in (a) through (m), the Applicant will comply with California's Fair Employment and Housing Act (FEHA). FEHA prohibits harassment and discrimination in employment because of ancestry, familial status, race, color, religious creed (including religious dress and grooming practices), sex (which includes pregnancy, childbirth, breastfeeding and medical conditions related to pregnancy, childbirth or breastfeeding), gender, gender identity, gender expression, sexual orientation, marital status, national origin, ancestry, mental and physical disability, genetic information, medical condition, age, pregnancy, denial of medical and family care leave, or pregnancy disability leave (California Government Code §§12940, 12945, 12945.2), military and veteran status, and/or retaliation for protesting illegal discrimination related to one of these categories, or for reporting patient abuse in tax supported institutions.

### **6. Drug-Free Workplace**

As required by the Drug-Free Workplace Act of 1988 (41 U.S.C. § 701 et seq.), the Applicant certifies that it will maintain a drug-free workplace and a drug-free awareness program as outlined in the Act.

### **7. Environmental Standards**

The Applicant will comply with state and federal environmental standards, which may be prescribed pursuant to the following, as applicable:

- (a) California Environmental Quality Act (CEQA) (California Public Resources Code §§ 21000- 21177), to include coordination with the city or county planning agency;
- (b) CEQA Guidelines (California Code of Regulations, Title 14, Division 6, Chapter 3, §§ 15000- 15387);
- (c) Federal Clean Water Act (CWA) (33 U.S.C. § 1251 et seq.), which establishes the basic structure for regulating discharges of pollutants into the waters of the United States and regulating quality standards for surface waters;
- (d) Federal Clean Air Act of 1955 (42 U.S.C. § 7401) which regulates air emissions from stationary and mobile sources;

## EXHIBIT A

- (e) Institution of environmental quality control measures under the National Environmental Policy Act (NEPA) of 1969 (P.L. 91-190); the Council on Environmental Quality Regulations for Implementing the Procedural Provisions of NEPA; and Executive Order 12898 which focuses on the environmental and human health effects of federal actions on minority and low-income populations with the goal of achieving environmental protection for all communities;
- (f) Evaluation of flood hazards in floodplains in accordance with Executive Order 11988;
- (g) Executive Order 11514 which sets forth national environmental standards;
- (h) Executive Order 11738 instituted to assure that each federal agency empowered to enter into contracts for the procurement of goods, materials, or services and each federal agency empowered to extend federal assistance by way of grant, loan, or contract shall undertake such procurement and assistance activities in a manner that will result in effective enforcement of the Clean Air Act and the Federal Water Pollution Control Act Executive Order 11990 which requires preservation of wetlands;
- (i) The Safe Drinking Water Act of 1974, (P.L. 93-523);
- (j) The Endangered Species Act of 1973, (P.L. 93-205);
- (k) Assurance of project consistency with the approved state management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.);
- (l) Conformity of Federal Actions to State (Clear Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1974, as amended (42 U.S.C. §§7401 et seq.);
- (m) Wild and Scenic Rivers Act of 1968 (16 U.S.C. § 1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

The Applicant shall not be: 1) in violation of any order or resolution promulgated by the State Air Resources Board or an air pollution district; 2) subject to a cease and desist order pursuant to § 13301 of the California Water Code for violation of waste discharge requirements or discharge prohibitions; or 3) determined to be in violation of federal law relating to air or water pollution.

### **8. Audits**

For subrecipients expending \$750,000 or more in federal grant funds annually, the Applicant will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and Title 2 of the Code of Federal Regulations, Part 200, Subpart F Audit Requirements.

### **9. Access to Records**

In accordance with 2 C.F.R. § 200.336, the Applicant will give the awarding agency, the Comptroller General of the United States and, if appropriate, the state, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award. The Applicant will require any subrecipients, contractors, successors, transferees and assignees to acknowledge and agree to comply with this provision.

## **EXHIBIT A**

### **10. Conflict of Interest**

The Applicant will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

### **11. Financial Management**

#### False Claims for Payment

The Applicant will comply with 31 U.S.C §§ 3729-3733 which sets forth that no subgrantee, recipient, or subrecipient shall submit a false claim for payment, reimbursement or advance.

### **12. Reporting - Accountability**

The Applicant agrees to comply with applicable provisions of the Federal Funding Accountability and Transparency Act (FFATA) (P.L. 109-282), specifically (a) the reporting of subawards obligating \$25,000 or more in federal funds and (b) executive compensation data for first-tier subawards. This includes the provisions of FFATA, which includes requirements for executive compensation, and also requirements implementing the Act for the non-federal entity at 2 C.F.R. Part 25 Financial Assistance Use of Universal Identifier and Central Contractor Registration and 2 C.F.R. Part 170 Reporting Subaward and Executive Compensation Information.

### **13. Whistleblower Protections**

The Applicant also must comply with statutory requirements for whistleblower protections at 10 U.S.C. § 2409, 41 U.S.C. § 4712, and 10 U.S.C. § 2324, 41 U.S.C. § 4304 and § 4310.

### **14. Human Trafficking**

The Applicant will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act of 2000, as amended (22 U.S.C. § 7104) which prohibits grant award recipients or a subrecipient from: (1) engaging in trafficking in persons during the period of time that the award is in effect; (2) procuring a commercial sex act during the period of time that the award is in effect; or (3) using forced labor in the performance of the award or subawards under the award.

### **15. Labor Standards**

The Applicant will comply with the following federal labor standards:

- (a) The Davis-Bacon Act (40 U.S.C. §§ 276a to 276a-7), as applicable, and the Copeland Act (40 U.S.C. § 3145 and 18 U.S.C. § 874) and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§ 327-333), regarding labor standards for federally-assisted construction contracts or subcontracts, and
- (b) The Federal Fair Labor Standards Act (29 U.S.C. § 201 et al.) as they apply to employees of institutes of higher learning (IHE), hospitals and other non-profit organizations.

## **EXHIBIT A**

### **16. Worker's Compensation**

The Applicant must comply with provisions which require every employer to be insured to protect workers who may be injured on the job at all times during the performance of the work of this Agreement, as per the workers compensation laws set forth in California Labor Code §§ 3700 et seq.

### **17. Property-Related**

If applicable to the type of project funded by this federal award, the Applicant will:

- (a) Comply with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of federal participation in purchase;
- (b) Comply with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires subrecipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is \$10,000 or more;
- (c) Assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. § 470), Executive Order 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §469a-1 et seq.); and
- (d) Comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. § 4831 and 24 CFR Part 35) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.

### **18. Certifications Applicable Only to Federally-Funded Construction Projects**

For all construction projects, the Applicant will:

- (a) Not dispose of, modify the use of, or change the terms of the real property title or other interest in the site and facilities without permission and instructions from the awarding agency. Will record the federal awarding agency directives and will include a covenant in the title of real property acquired in whole or in part with federal assistance funds to assure nondiscrimination during the useful life of the project;
- (b) Comply with the requirements of the awarding agency with regard to the drafting, review and approval of construction plans and specifications; and
- (c) Provide and maintain competent and adequate engineering supervision at the construction site to ensure that the complete work conforms with the approved plans and specifications and will furnish progressive reports and such other information as may be required by the assistance awarding agency or State.

## **EXHIBIT A**

### **19. Use of Cellular Device While Driving is Prohibited**

Applicants are required to comply with California Vehicle Code sections 23123 and 23123.5. These laws prohibit driving motor vehicle while using an electronic wireless communications device to write, send, or read a text-based communication. Drivers are also prohibited from the use of a wireless telephone without hands-free listening and talking, unless to make an emergency call to 911, law enforcement, or similar services.

### **20. California Public Records Act and Freedom of Information Act**

The Applicant acknowledges that all information submitted in the course of applying for funding under this program, or provided in the course of an entity's grant management activities that are under Federal control, is subject to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and the California Public Records Act, California Government Code section 6250 et seq. The Applicant should consider these laws and consult its own State and local laws and regulations regarding the release of information when reporting sensitive matters in the grant application, needs assessment, and strategic planning process.

### **HOMELAND SECURITY GRANT PROGRAM - PROGRAM SPECIFIC ASSURANCES / CERTIFICATIONS**

#### **21. Reporting Accusations and Findings of Discrimination**

If during the past three years the recipient has been accused of discrimination on any basis the recipient must provide a list of all such proceedings, pending or completed, including outcome and copies of settlement agreements to the DHS Financial Assistance Office and the DHS Office for Civil Rights and Civil Liberties (CRCL) by e-mail at [CRCL@hq.dhs.gov](mailto:CRCL@hq.dhs.gov) or by mail at U.S. Department of Homeland Security, Office for Civil Rights and Civil Liberties, Building 410, Mail Stop #0190, Washington, D.C. 20528.

In the courts or administrative agencies make a finding of discrimination on grounds of race, color, national origin (including LEP), sex, age, disability, religion, or familial status against the recipient, or the recipients settle a case or matter alleging such discrimination, recipients must forward a copy of the complaint and findings to the DHS Financial Assistance Office and the CRCL by e-mail or mail at the addresses listed above.

The United States has the right to seek judicial enforcement of these obligations.

#### **22. Acknowledgment of Federal Funding from DHS**

All recipients must acknowledge their use of federal funding when issuing statements, press releases, requests for proposals, bid invitations, and other documents describing projects or programs funded in whole or in part with federal funds.

#### **23. Activities Conducted Abroad**

All recipients must ensure that project activities carried on outside the United States are coordinated as necessary with appropriate government authorities and that appropriate licenses, permits, or approvals are obtained.

## **EXHIBIT A**

### **24. Best Practices for Collection and Use of Personally Identifiable Information (PII)**

DHS defines personally identifiable information (PII) as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual. All recipients who collect PII are required to have a publicly-available privacy policy that describes standards on the usage and maintenance of PII they collect. Recipients may also find the DHS Privacy Impact Assessments: Privacy Guidance and Privacy template a useful resource respectively.

### **25. Copyright**

All recipients must affix the applicable copyright notices of 17 U.S.C. §§ 401 or 402 and an acknowledgement of U.S. Government sponsorship (including the award number) to any work first produced under federal financial assistance awards.

### **26. Duplication of Benefits**

Any cost allocable to a particular federal financial assistance award provided for in 2 C.F.R. Part 200, Subpart E may not be charged to other federal financial assistance awards to overcome fund deficiencies, to avoid restrictions imposed by federal statutes, regulations, or federal financial assistance award terms and conditions, or for other reasons. However, these prohibitions would not preclude recipients from shifting costs that are allowable under two or more awards in accordance with existing federal statutes, regulations, or the federal financial assistance award terms and conditions.

### **27. Energy Policy and Conservation Act**

All recipients must comply with the requirements of 42 U.S.C. § 6201 which contain policies relating to energy efficiency that are defined in the state energy conservation plan issued in compliance with this Act.

### **28. Federal Debt Status**

All recipients are required to be non-delinquent in their repayment of any federal debt. Examples of relevant debt include delinquent payroll and other taxes, audit disallowances, and benefit overpayments. See OMB Circular A-129.

### **29. Fly America Act of 1974**

All recipients must comply with Preference for U.S. Flag Air Carriers: (air carriers holding certificates under 49 U.S.C. § 41102) for international air transportation of people and property to the extent that such service is available, in accordance with the International Air Transportation Fair Competitive Practices Act of 1974 (49 U.S.C. § 40118) and the interpretative guidelines issued by the Comptroller General of the United States in the March 31, 1981, amendment to Comptroller General Decision B-138942.

### **30. Hotel and Motel Fire Safety Act of 1990**

In accordance with Section 6 of the Hotel and Motel Fire Safety Act of 1990, all Applicants must ensure that all conference, meeting, convention, or training space funded in whole or in part with federal funds complies with the fire prevention and control guidelines of the Federal Fire Prevention and Control Act of 1974, as amended, 15 U.S.C. § 2225a.

## **EXHIBIT A**

### **31. Non-supplanting Requirement**

All recipients who receive federal financial assistance awards made under programs that prohibit supplanting by law must ensure that federal funds do not replace (supplant) funds that have been budgeted for the same purpose through non-federal sources.

### **32. Patents and Intellectual Property Rights**

Unless otherwise provided by law, recipients are subject to the Bayh-Dole Act, Pub. L. No. 96-517, as amended, and codified in 35 U.S.C. § 200 et seq. All recipients are subject to the specific requirements governing the development, reporting, and disposition of rights to inventions and patents resulting from financial assistance awards located at 37 C.F.R. Part 401 and the standard patent rights clause located at 37 C.F.R. § 401.14.

### **33. SAFECOM**

All recipients who receive federal financial assistance awards made under programs that provide emergency communication equipment and its related activities must comply with the SAFECOM Guidance for Emergency Communication Grants, including provisions on technical standards that ensure and enhance interoperable communications.

### **34. Terrorist Financing**

All recipients must comply with Executive Order 13224 and U.S. law that prohibit transactions with, and the provisions of resources and support to, individuals and organizations associated with terrorism. Recipients are legally responsible to ensure compliance with the Order and laws.

### **35. Reporting of Matters Related to Recipient Integrity and Performance**

If the total value of the recipient's currently active grants, cooperative agreements, and procurement contracts from all federal assistance offices exceeds \$10,000,000 for any period of time during the period of performance of this federal financial assistance award, you must comply with the requirements set forth in the government-wide Award Term and Condition for Recipient Integrity and Performance Matters located at 2 C.F.R. Part 200, Appendix XII, the full text of which is incorporated here by reference in the award terms and conditions.

### **36. USA Patriot Act of 2001**

All recipients must comply with requirements of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), which amends 18 U.S.C. §§ 175–175c.

### **37. Use of DHS Seal, Logo, and Flags**

All recipients must obtain permission from their DHS Financial Assistance Office, prior to using the DHS seal(s), logos, crests or reproductions of flags or likenesses of DHS agency officials, including use of the United States Coast Guard seal, logo, crests or reproductions of flags or likenesses of Coast Guard officials.

## **EXHIBIT A**

### **IMPORTANT**

The purpose of the assurance is to obtain federal and state financial assistance, including any and all federal and state grants, loans, reimbursement, contracts, etc. The Applicant recognizes and agrees that state financial assistance will be extended based on the representations made in this assurance. This assurance is binding on the Applicant, its successors, transferees, assignees, etc. Failure to comply with any of the above assurances may result in suspension, termination, or reduction of grant funds.

All appropriate documentation, as outlined above, must be maintained on file by the Applicant and available for Cal OES or public scrutiny upon request. Failure to comply with these requirements may result in suspension of payments under the grant or termination of the grant or both and the subrecipient may be ineligible for award of any future grants if the Cal OES determines that any of the following has occurred: (1) the recipient has made false certification, or (2) violates the certification by failing to carry out the requirements as noted above.

All of the language contained within this document must be included in the award documents for all subawards at all tiers. All recipients are bound by the Department of Homeland Security Standard Terms and Conditions 2018, Version 8.1, hereby incorporated by reference, which can be found at: <https://www.dhs.gov/publication/fy15-dhs-standard-terms-and-conditions>.

**The undersigned represents that he/she is authorized to enter into this agreement for and on behalf of the Applicant.**

Subrecipient: \_\_\_\_\_

Signature of Authorized Agent: \_\_\_\_\_

Printed Name of Authorized Agent: \_\_\_\_\_

Title: \_\_\_\_\_ Date: \_\_\_\_\_

## **EXHIBIT B**

### **Federally-Funded Services**

(Pursuant to Appendix II, 2 CFR Part 200)

**(1) Equal Employment Opportunity.** Except as otherwise provided under 41 CFR Part 60, if this Agreement meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3, then during the performance of this Agreement, the SUBRECIPIENT agrees as follows: (1) The SUBRECIPIENT will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The SUBRECIPIENT will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following: Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The SUBRECIPIENT agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.(2) The SUBRECIPIENT will, in all solicitations or advertisements for employees placed by or on behalf of the SUBRECIPIENT, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.(3) The SUBRECIPIENT will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the SUBRECIPIENT'S legal duty to furnish information.(4) The SUBRECIPIENT will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the SUBRECIPIENT'S commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.(5) The SUBRECIPIENT will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.(6) The SUBRECIPIENT will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.(7) In the event of the SUBRECIPIENT'S noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this Agreement may be canceled, terminated, or suspended in whole or in part and the SUBRECIPIENT may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.(8) The SUBRECIPIENT will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The SUBRECIPIENT will take such action with respect to any subcontract or purchase order as the COUNTY may direct as a means of enforcing such provisions, including sanctions for noncompliance: *Provided*, however, that in the event SUBRECIPIENT becomes involved in, or is threatened with, litigation with a sub-contractor or vendor as a result of such direction

## **EXHIBIT B**

by the COUNTY, then the SUBRECIPIENT may request the United States to enter into such litigation to protect the interests of the United States. The COUNTY further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work.

The COUNTY agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance. The COUNTY further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the COUNTY agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the COUNTY under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from the COUNTY; and refer the case to the Department of Justice for appropriate legal proceedings.

The SUBRECIPIENT and each of its subcontractors shall include this equal opportunity clause in each of its subcontracts.

**(2) Davis-Bacon Act, as amended (40 U.S.C. 3141–3148).** If this Agreement involves payment for construction services in excess of \$2,000, then the SUBRECIPIENT must comply with the Davis-Bacon Act (40 U.S.C. 3141–3144, and 3146–3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the Davis-Bacon Act, the SUBRECIPIENT is required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the U.S. Secretary of Labor. In addition, the SUBRECIPIENT is required to pay wages not less than once a week. The COUNTY must provide SUBRECIPIENT with a copy of the current prevailing wage determination issued by the U.S. Department of Labor with respect to the services to be provided under the subject Agreement. The SUBRECIPIENT'S execution of the subject Agreement constitutes the SUBRECIPIENT'S acceptance of the wage determination. The COUNTY must report all suspected or reported violations to the Federal awarding agency.

**(3) Copeland "Anti- Kickback" Act (40 U.S.C. 3145).** SUBRECIPIENT must comply with the Copeland "Anti- Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). Under the Copeland "Anti- Kickback" Act, the SUBRECIPIENT and all subcontractors are prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The COUNTY must report all suspected or reported violations to the Federal awarding agency.

**(4) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701–3708).** If this Agreement

## **EXHIBIT B**

involves payments for services in excess of \$100,000 that include the employment of mechanics or laborers, then the SUBRECIPIENT must comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, the SUBRECIPIENT is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

**(5) Rights to Inventions Made Under a Contract or Agreement.** If the Federal award supporting payments for services under this Agreement meets the definition of “funding agreement” under 37 CFR § 401.2 (a) and the Agreement is with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that “funding agreement,” then the COUNTY and the SUBRECIPIENT must comply with the requirements of 37 CFR Part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any implementing regulations issued by the awarding agency.

**(6) Clean Air Act (42 U.S.C. 7401–7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251–1387), as amended.** If this Agreement involves payments for services in excess of \$150,000, then the SUBRECIPIENT must comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251–1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

**(7) Debarment and Suspension (Executive Orders 12549 and 12689).** By execution of this Agreement, SUBRECIPIENT certifies to the COUNTY that it is not a party listed on the government-wide exclusions list in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), “Debarment and Suspension,” and is not debarred, suspended, or otherwise excluded from the award of a federally-supported contract under statutory or regulatory authority other than Executive Order 12549.

**(8) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352).** If this Agreement involves payments for services in excess of \$100,000, then by execution of this Agreement, the SUBRECIPIENT certifies to the COUNTY that it will not and has not used Federally-appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. The SUBRECIPIENT must also disclose to the COUNTY in writing any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award.

**(9) Procurement of recovered materials.** Pursuant to 2 CFR § 200.322, COUNTY and SUBRECIPIENT must comply with section 6002 of the Federal Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that

## **EXHIBIT B**

contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

**(10) Records Retention and Access.** Pursuant to 2 CFR §§ 200.333 through 200.337, the following provisions regarding Records Retention and Access will apply to this Agreement:

(a) Retention requirements for records. SUBRECIPIENT must retain all financial records, supporting documents, statistical records, and all other of its records pertinent to this Agreement for a period of three years from the date of submission of the final expenditure report or, for Federal awards that are renewed quarterly or annually, from the date of the submission of the quarterly or annual financial report, respectively, as reported to the Federal awarding agency or COUNTY. The only exceptions to the 3 year limit are the following:

(i) If any litigation, claim, or audit is started before the expiration of the 3-year period, then the records must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken.

(ii) When the SUBRECIPIENT is notified in writing by the COUNTY or Federal awarding agency, cognizant agency for audit, oversight agency for audit, or cognizant agency for indirect costs to extend the retention period.

(iii) Records for real property and equipment acquired with Federal funds must be retained for 3 years after final disposition.

(iv) When records are transferred to or maintained by the COUNTY, or Federal awarding agency, the 3-year retention requirement is not applicable to the SUBRECIPIENT.

(v) Records for program income transactions after the period of performance. In some cases recipients must report program income after the period of performance. Where there is such a requirement, the retention period for the records pertaining to the earning of the program income starts from the end of the SUBRECIPIENT'S fiscal year in which the program income is earned.

(vi) Indirect cost rate proposals and cost allocations plans. This paragraph applies to the following types of documents and their supporting records: indirect cost rate computations or proposals, cost allocation plans, and any similar accounting computations of the rate at which a particular group of costs is chargeable (such as computer usage chargeback rates or composite fringe benefit rates).

1. *If submitted for negotiation.* If the proposal, plan, or other computation is required to be submitted to the COUNTY or the Federal Government to form the basis for negotiation of the rate, then the 3-year retention period for its supporting records starts from the date of such submission.

2. *If not submitted for negotiation.* If the proposal, plan, or other computation is not required to be submitted to the COUNTY or Federal Government for negotiation purposes, then the 3-year retention period for the proposal, plan, or computation and its supporting records starts from the end of the fiscal year (or other accounting period) covered by the proposal, plan, or other computation.

(b) Methods for collection, transmission and storage of information. In accordance with the May 2013 Executive Order on Making Open and Machine Readable the New Default for Government Information, the Federal awarding agency and the SUBRECIPIENT should, whenever practicable, collect, transmit, and store Federal award-related information in open and machine readable formats rather than in closed formats or on paper. The Federal awarding agency or COUNTY must always provide or accept paper versions of Federal award-related information to and from the SUBRECIPIENT upon request. If paper copies are submitted, the Federal awarding agency or COUNTY must not require more than an

## **EXHIBIT B**

original and two copies. When original records are electronic and cannot be altered, there is no need to create and retain paper copies. When original records are paper, electronic versions may be substituted through the use of duplication or other forms of electronic media provided that they are subject to periodic quality control reviews, provide reasonable safeguards against alteration, and remain readable.

*(c) Access to records.*

(i) Records of SUBRECIPIENT. The Federal awarding agency, Inspectors General, the Comptroller General of the United States, the State of California, and the COUNTY, or any of their authorized representatives, must have the right of access to any documents, papers, or other records of the SUBRECIPIENT which are pertinent to the Federal award, in order to make audits, examinations, excerpts, and transcripts. The right also includes timely and reasonable access to the SUBRECIPIENT'S personnel for the purpose of interview and discussion related to such documents.

(ii) Only under extraordinary and rare circumstances would such access include review of the true name of victims of a crime. Routine monitoring cannot be considered extraordinary and rare circumstances that would necessitate access to this information. When access to the true name of victims of a crime is necessary, appropriate steps to protect this sensitive information must be taken by both the SUBRECIPIENT and the Federal awarding agency or COUNTY. Any such access, other than under a court order or subpoena pursuant to a bona fide confidential investigation, must be approved by the head of the Federal awarding agency or delegate.

(iii) Expiration of right of access. The rights of access in this section are not limited to the required retention period but last as long as the records are retained. Federal awarding agencies and COUNTY must not impose any other access requirements upon SUBRECIPIENT.

**8592.5.** (a) Except as provided in subdivision (c), a state department that purchases public safety radio communication equipment shall ensure that the equipment purchased complies with applicable provisions of the following:

(1) The common system standards for digital public safety radio communications commonly referred to as the "Project 25 Standard," as that standard may be amended, revised, or added to in the future jointly by the Associated Public-Safety Communications Officials, Inc., National Association of State Telecommunications Directors and agencies of the federal **government**, commonly referred to as "APCO/NASTD/FED."

(2) The operational and functional requirements delineated in the Statement of Requirements for Public Safety Wireless Communications and Interoperability developed by the SAFECOM Program under the United States Department of Homeland Security.

(b) Except as provided in subdivision (c), a local first response agency that purchases public safety radio communication equipment, in whole or in part, with state funds or federal funds administered by the state, shall ensure that the equipment purchased complies with paragraphs (1) and (2) of subdivision (a).

(c) Subdivision (a) or (b) shall not apply to either of the following:

(1) Purchases of equipment to operate with existing state or local communications systems where the latest applicable standard will not be compatible, as verified by the Telecommunications Division of the Department of General Services.

(2) Purchases of equipment for existing statewide low-band public safety communications systems.

(d) This section may not be construed to require an affected state or local governmental agency to compromise its immediate mission or ability to function and carry out its existing responsibilities.





**CISA**  
CYBER+INFRASTRUCTURE



# SAFECOM Guidance on Emergency Communications Grants

---

Fiscal Year 2020

## A Message to Stakeholders

---

On behalf of the Cybersecurity and Infrastructure Security Agency (CISA), I am releasing the *Fiscal Year 2020 SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)*. This document is updated annually to provide current information on emergency communications policies, eligible costs, best practices, and technical standards for state, local, tribal, and territorial grant recipients investing federal funds in emergency communications projects.

The *SAFECOM Guidance* aligns with the *National Emergency Communications Plan* (NECP), recently updated in 2019, which emphasizes the need to enhance governance structures, plans, and protocols that enable the emergency response community to communicate and share information under all circumstances. It aims to maximize the use of all communications capabilities available to public safety officials—voice, video, and data—and to ensure the security of data and information exchange. To accomplish this, grant recipients must engage the whole community in preparedness activities. Similarly, the *SAFECOM Guidance* addresses the rapidly evolving emergency communications ecosystem and encourages grant recipients to support the concepts and recommendations within the NECP.

The Administration, Office of Management and Budget, and federal grant program offices recognize the *SAFECOM Guidance* as the primary guidance on emergency communications grants. Since 2015, the Department of Homeland Security has required its grant recipients investing in emergency communications to comply with *SAFECOM Guidance*. All grant applicants are encouraged to coordinate with their statewide governance bodies and emergency communications leaders (e.g., Statewide Interoperability Coordinators) to ensure projects support the state, local, tribal, or territory's strategy to improve interoperable emergency communications. In addition, grant applicants should work with public and private entities, and across jurisdictions and disciplines, to assess needs, plan projects, coordinate resources, and improve response through cross-training and joint exercises. These coordination efforts are important to ensure interoperability remains a top priority.

The *SAFECOM Guidance* encourages grant applicants to participate, support, and invest in planning activities that will help states or territories prepare for deployment of new emergency communications systems or technologies. At the same time, there is a need to sustain current land mobile radio (LMR) systems into the foreseeable future. Grant recipients should continue enhancing governance and leadership, developing plans and procedures, conducting training and exercises, and investing in standards-based equipment to sustain LMR capabilities, while concurrently planning for the integration and deployment of new technologies. Grant recipients must also consider cybersecurity risks across all capabilities when planning operable, interoperable, and continuity of communications.

As in previous years, CISA developed the *SAFECOM Guidance* in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators. CISA also consulted federal partners and the Emergency Communications Preparedness Center to ensure emergency communications policies are coordinated and consistent across the Federal Government. Grant applicants are encouraged to reference this document when developing emergency communications investments for federal funding, and to direct any questions to my office at [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov).



Vincent DeLaurentis  
Acting Assistant Director for Emergency Communications  
Cybersecurity and Infrastructure Security Agency  
U.S. Department of Homeland Security

## **Contents**

---

A Message to Stakeholders.....	2
Contents .....	3
1. Introduction .....	4
1.1 Purpose of SAFECOM Guidance .....	4
1.2 Report Methodology .....	5
1.3 Use of SAFECOM Guidance.....	6
1.4 Key Changes and Updates .....	8
2. Emergency Communications Priorities.....	9
2.1 Priority 1: Governance and Leadership .....	9
2.2 Priority 2: Planning and Procedures .....	10
2.3 Priority 3: Training, Exercises, and Evaluation .....	12
2.4 Priority 4: Activities that Enhance Communications Coordination.....	13
2.5 Priority 5: Standards-based Technology and Infrastructure.....	14
2.6 Priority 6: Cybersecurity.....	16
3. Before Applying.....	17
3.1 Review the NECP and SCIP .....	17
3.2 Coordinate with Statewide Emergency Communications Leaders.....	17
3.3 Recognize Changes in the Emergency Communications Ecosystem .....	17
3.4 Understand Federal Grant Requirements and Restrictions .....	23
4. Eligible Activities.....	26
4.1 Personnel.....	26
4.2 Planning and Organization.....	27
4.3 Training.....	30
4.4 Exercises .....	31
4.5 Equipment.....	32
5. Emergency Communications Systems and Capabilities .....	36
6. Grants Management Best Practices .....	37
7. Funding Sources.....	38
Appendix A – Acronym List.....	A-1
Appendix B – Technology and Equipment Standards and Resources.....	B-1
Appendix C – Emergency Communications Resources .....	C-1
Appendix D – Compliance Requirements for DHS Grants .....	D-1

## 1. Introduction

---

The Department of Homeland Security (DHS) is mandated to administer responsibilities and authorities relating to the SAFECOM Program. Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for developing coordinated guidance for federal grant programs for public safety communications.<sup>1</sup> As a result, CISA develops the annual *SAFECOM Guidance on Emergency Communications Grants* (*SAFECOM Guidance*) as a reference guide for entities applying for federal financial assistance for emergency communications projects. While only entities funding emergency communications projects with DHS grant funding are required to comply with *SAFECOM Guidance* (see Appendix D), all entities are highly encouraged to follow the recommendations within this document to ensure interoperable, resilient, and fully effective communications.

The *SAFECOM Guidance* provides general information on eligible activities, technical standards, and other terms and conditions that are common to most federal emergency communications grants.<sup>2</sup> It aims to ensure that policies and standards across federal grant programs provide a consistent approach to improving emergency communications nationwide. The *SAFECOM Guidance* achieves this consistency by aligning recommendations with the Nation's strategic plan for emergency communications, entitled the *National Emergency Communications Plan* (NECP).<sup>3</sup>

SAFECOM is a public safety-driven program sponsored by CISA, which develops policy, guidance, and future efforts by drawing on SAFECOM member expertise and recommendations. The DHS Science and Technology Directorate also supports SAFECOM-related research, development, testing, evaluation, as well as the acceleration of standards. SAFECOM works to build partnerships among all levels of government, linking the strategic planning, technical support, and implementation needs of the emergency response community with federal, state, local, tribal, and territorial governments, to improve communications.

Additionally, CISA consulted members of the Emergency Communications Preparedness Center, which coordinates roles and activities of agencies across the Federal Government to improve interoperable public safety and emergency response communications. It consists of 14 federal departments and agencies representing the government's broad role in improving coordination of emergency communications efforts, including information sharing, planning, regulation, policy, operations, grants, and technical assistance. Together, SAFECOM members and federal partners coordinate on emergency communications policy and standards to ensure projects are compatible, interoperable, and most importantly, meet needs of end-users.

### 1.1 Purpose of SAFECOM Guidance

The *SAFECOM Guidance* provides guidance to grant recipients<sup>4</sup> on:

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

---

<sup>1</sup> 6 U.S.C. § 571(c)(2) and 6 U.S.C. § 574.

<sup>2</sup> Federal financial assistance includes grants, loans, cooperative agreements, and other funds provided by the Federal Government. For this document, these terms are used interchangeably unless otherwise indicated.

<sup>3</sup> For more information on the NECP, see: <https://www.cisa.gov/necp>.

<sup>4</sup> In accordance with Title 2 of the Code of Federal Regulations (CFR) 200, the terms "recipient" and "sub-recipient" is defined as a non-federal entity that receives a federal award directly from a federal awarding agency to carry out an activity under a federal program.

The *SAFECOM Guidance* is designed to promote and align with the national vision established in the NECP. CISA published a second update to the NECP in September 2019 that builds upon revisions made in 2014, while also positioning the NECP to maintain relevance into the future. Updates to the NECP goals and objectives aim to enhance emergency communications capabilities at all levels of government in coordination with the private sector, nongovernmental organizations, and communities across the Nation. The plan's success relies on the whole community embracing the NECP goals and objectives, and most importantly implementing them. Critical components for advancing emergency communications fall under three national priorities:

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

Recommendations within the *SAFECOM Guidance* are intended to help state, local, tribal, and territorial stakeholders develop projects that meet critical emergency communications needs defined in the NECP and their Statewide Communication Interoperability Plan (SCIP).<sup>5</sup> Best practices and technical standards located within the *SAFECOM Guidance* help ensure federally-funded investments are interoperable, fully effective and reliable, and support national policies. However, not all guidance is applicable to all grant programs. Grants funding emergency communications are administered by numerous federal agencies and are subject to various statutory and programmatic requirements. As a result, grant applicants and recipients should review specific grant guidance carefully to ensure their proposed activities are eligible, and all standards, terms, and conditions required by the program are met.<sup>6</sup>

## 1.2 Report Methodology

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

- Emergency Communications Preparedness Center (ECPC) Grants Focus Group<sup>7</sup>
- Federal Communications Commission (FCC), Public Safety and Homeland Security Bureau (PSHSB)
- SAFECOM<sup>8</sup> and the National Council of Statewide Interoperability Coordinators (NCSWIC)
- U.S. Department of Commerce
  - First Responder Network Authority (FirstNet Authority)
  - National Institute of Standards and Technology (NIST)
  - National Telecommunications and Information Administration (NTIA)
- U.S. Department of Homeland Security
  - Federal Emergency Management Agency (FEMA)
  - Integrated Public Alert and Warning System (IPAWS)
  - Science and Technology Directorate, Office for Interoperability and Compatibility
- U.S. Department of Justice, Office of Justice Programs
- U.S. Department of Transportation, National Highway Traffic Safety Administration (NHTSA)

---

<sup>5</sup> For information on SCIPs, see: <https://www.cisa.gov/statewide-communication-interoperability-plans>.

<sup>6</sup> For the purposes of this document, “grant guidance” may include Notices of Funding Opportunity, Grant Notices, Grant Applications, and other formal notices of grants and federal financial assistance programs.

<sup>7</sup> The ECPC Grants Focus Group is comprised of grant officers, program administrators, and communications experts representing the 14 federal agencies that participate in the ECPC.

<sup>8</sup> For a list of SAFECOM members, see: <http://www.dhs.gov/safecom/membership>.

### 1.3 Use of SAFECOM Guidance

The *SAFECOM Guidance* should be used during planning, development, and implementation of emergency communications projects and in conjunction with other planning documents. Before proposing projects for funding, prospective applicants are encouraged to read the NECP, federal and state preparedness documents such as statewide plans and reports, and the *SAFECOM Guidance* to ensure projects support federal, state, local, tribal, and territorial plans for improving emergency communications. Table 1 provides a list of essential resources available to recipients.

**Table 1. Essential Resources for Emergency Communications Grant Recipients**

Resources	Descriptions
<b>National Emergency Communication Plan</b>	The NECP is the Nation's strategic plan that promotes communication and information sharing across all levels of government, jurisdictions, disciplines, and organizations for all threats and hazards, as needed and when authorized. It provides information and guidance to those that plan for, coordinate, invest in, and use communications to support response operations. Grant applicants are encouraged to read the NECP to understand the national strategy, and to ensure investments support the goals and objectives. The NECP is available at: <a href="https://www.cisa.gov/necp">https://www.cisa.gov/necp</a> .
<b>Statewide Communication Interoperability Plan</b>	The SCIP contains the state, territory, or tribal government's strategy to improve emergency communications. States and territories were required to develop and submit a SCIP to DHS by December 2008 and required to submit reports annually on the progress of the state or territory in implementing its SCIP. Many federal grants funding emergency communications require grant applicants to align projects to needs identified in SCIPs. Grant recipients and sub-recipients should review the SCIP for their state/territory and work with their Statewide Interoperability Coordinator (SWIC) to ensure investments support statewide plans to improve communications. To find your state's SCIP, please contact your SWIC. Contact information for SWICs can be found on the NCSWIC membership page: <a href="https://www.dhs.gov/safecom/ncswic-membership">https://www.dhs.gov/safecom/ncswic-membership</a> .
<b>SAFECOM Website</b>	The SAFECOM website provides information and resources for public safety agencies developing emergency communications projects. For the most recent <i>SAFECOM Guidance</i> and list of grants funding emergency communications, see the SAFECOM website at: <a href="https://www.dhs.gov/safecom/funding">https://www.dhs.gov/safecom/funding</a> .
<b>IPAWS Website</b>	This website contains information on IPAWS's capabilities, who can use IPAWS to send alerts and warnings, and organizations that work with the IPAWS Program Management Office to support public alerts and warnings. IPAWS is accessed through software that meets IPAWS system requirements. There is no cost to send messages through IPAWS, although there may be costs associated with acquiring compatible alert origination software. Grant recipients are encouraged to invest in alerting software. IPAWS is not mandatory and does not replace existing methods of alerting, but instead complements existing systems and offers new capabilities to deliver timely and actionable alerts. See the IPAWS website at: <a href="https://www.fema.gov/integrated-public-alert-warning-system">https://www.fema.gov/integrated-public-alert-warning-system</a> and information for alerting authorities at: <a href="https://www.fema.gov/alerting-authorities">https://www.fema.gov/alerting-authorities</a> .
<b>Office of Management and Budget (OMB) Grants Circulars</b>	Federal awards must adhere to the <i>Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards</i> at: <a href="https://www.govinfo.gov/app/details/CFR-2014-title2-vol1/CFR-2014-title2-vol1-part200">https://www.govinfo.gov/app/details/CFR-2014-title2-vol1/CFR-2014-title2-vol1-part200</a> . Grant applicants should reference specific Notices of Funding Opportunity to determine applicable requirements at: <a href="https://www.grants.gov">https://www.grants.gov</a> . Additional information is on the Chief Financial Officers Council website at: <a href="https://cfo.gov/grants">https://cfo.gov/grants</a> .

Resources	Descriptions
<b>Statewide Interoperability Coordinator</b>	States, territories, and tribal governments are encouraged to designate a full-time <b>SWIC</b> who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government. Grant applicants are strongly encouraged to coordinate project proposals with the SWIC to ensure projects support statewide efforts to improve emergency communications. DHS/FEMA requires all states and territories that use Homeland Security Grant Program funds to designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government. <a href="https://www.dhs.gov/safecom/ncswic-membership">https://www.dhs.gov/safecom/ncswic-membership</a> .
<b>State Leadership</b>	<p>As required as a condition of the State and Local Implementation Grant Program (SLIGP) 2.0, each State and Territory Governor designated an individual or body to serve as coordinator of implementation of the grant funds known as the <b>Single Point of Contact (SPOC)</b>. Grant recipients are encouraged to consult with the appropriate point of contact or governance body for their state or territory when engaging in public safety broadband activities.</p>
	<p>The <b>State Emergency Management Agency Director</b> is responsible for ensuring the state or territory is prepared to deal with any type of emergency, as well as coordinating statewide incident response. This includes collaborating with appropriate statewide representatives for critical capabilities, such as emergency communications, statewide 911 communications, and public alerting.</p> <p><b>State Information Technology and Security Officials</b>, including a state or territory's Chief Information Officer, Chief Technology Officer, and Chief Information Security Officer manage key information technology (IT) initiatives, including IT procurement, security, and IT planning and budgeting.</p> <p>The <b>911 Administrator</b> manages the state or territory's 911 functions as determined by state legislation. The official title and role of this position may vary. Grant recipients are encouraged to coordinate 911 projects with the Administrator to ensure projects support state or territory 911 efforts. To find your Administrator, refer to the National Association of State 911 Administrators at: <a href="http://www.nasna911.org/state-911-contacts">http://www.nasna911.org/state-911-contacts</a>.</p>
	<p>The <b>Homeland Security Director</b> coordinates the planning, development, and coordination of statewide policies developed in support of public and private organizations responsible for preventing terrorism, raising awareness, reducing vulnerabilities, responding to, and recovering from terrorist acts. To locate your Director or office, refer to: <a href="https://www.dhs.gov/state-homeland-security-contacts">https://www.dhs.gov/state-homeland-security-contacts</a>.</p>
<b>State Governance</b>	<p>The <b>Statewide Interoperability Governing Body (SIGB)</b> or <b>State Interoperability Executive Committee (SIEC)</b> serve as the primary steering group for the statewide interoperability strategy that seek to improve emergency response communications across the State through enhanced data and voice communications interoperability. SIGBs and SIECs include representatives from various jurisdictions, disciplines, as well as subject matter experts. To find the SIGB or SIEC for your state or territory, contact CISA at: <a href="mailto:ECD@cisa.dhs.gov">ECD@cisa.dhs.gov</a>.</p>
	<p>A <b>Broadband Working Group</b> serves as the governing body for state or territory planning activities for the FirstNet Authority. Many states are using their SIGB or SIEC for planning or have created an independent working group focused on public safety broadband. Grant recipients are encouraged to work with their respective group to ensure efforts do not conflict with the FirstNet Authority's planning and implementation of the Nationwide Public Safety Broadband Network (NPSBN).</p>
	<p>The <b>911 Advisory Board</b> works with the 911 Administrator to plan and coordinate state and local 911 efforts. The official title and role of this board vary. Grant applicants are encouraged to coordinate 911 projects with the Board to ensure projects support state or territory 911 efforts. To find your 911 Advisory Board, refer to State 911 Contacts page of the National Association of State 911 Administrators at: <a href="http://www.nasna911.org/state-911-contacts">http://www.nasna911.org/state-911-contacts</a>.</p>

## 1.4 Key Changes and Updates

This section highlights key changes to the *FY 2020 SAFECOM Guidance*:

- **Emergency Communications Priorities (Section 2).** This section reviews stakeholder-driven priorities aligned to the NECP goals and recommendations, including: 1) Governance and Leadership; 2) Planning and Procedures; 3) Training, Exercises, and Evaluation; 4) Activities that Enhance Communications Coordination; 5) Standards-based Technology and Infrastructure; and 6) Cybersecurity.

Based on lessons learned from recent federally-declared disasters, there is an urgent need to address communications survivability, resilience, and continuity. Rather than listing this as a separate priority, communications resilience and continuity should be viewed as a critical component across all priorities.

- **Before Applying (Section 3).** This section provides an overview of national policies, laws, and issues affecting emergency communications grants and the broader emergency communications ecosystem, as well as federal requirements and restrictions on funding that applicants should consider before applying.

New this year, the NECP update was released in September 2019. Congress directs CISA to complete a nationwide emergency communications baseline assessment every five years and to periodically update the NECP. Informed by the 2018 assessment results, updating the NECP keeps the plan forward-looking and accounts for changes in emergency communications policy, legislation, and technologies. NECP updates to the Nation's strategic plan for emergency communications have been incorporated throughout the *SAFECOM Guidance*.

- **Eligible Activities (Section 4).** This section includes a review of eligible costs commonly funded by federal grants, as well as guidance for applicants to address NECP strategic goals and recommendations. Grant applicants seeking to improve interoperable emergency communications are encouraged to allocate grant funding to these activities. However, applicants must consult the specific grant guidance they are applying for to confirm allowable costs, as all activities listed in this section may not be eligible for funding under all federal grant programs.
- **Emergency Communications Systems and Capabilities (Section 5).** This section provides an overview of emergency communications and the importance of deploying standards-based technology and equipment.
- **Grants Management Best Practices (Section 6).** This section provides best practices to ensure the effective implementation of grants and to establish the entity as a trusted steward of federal grant funding and a credible recipient of future grant funding.
- **Funding Sources (Section 7).** This section offers recommendations on how applicants should consider multiple funding sources, including traditional grants and other sources that may partially fund emergency communications projects.
- **Appendices.** The appendices include an acronym list (Appendix A), technical standards for emergency communications equipment (Appendix B), and resources recipients can reference when developing emergency communications projects (Appendix C).

In Appendix D, DHS has outlined specific requirements for DHS/FEMA recipients to comply with *SAFECOM Guidance*. These requirements are in accordance with the DHS Standard Terms and Conditions of preparedness grants.

## 2. Emergency Communications Priorities

---

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

- Priority 1: Governance and Leadership
- Priority 2: Planning and Procedures
- Priority 3: Training, Exercises, and Evaluation
- Priority 4: Activities that Enhance Communications Coordination
- Priority 5: Standards-Based Technology and Infrastructure
- Priority 6: Cybersecurity

### 2.1 Priority 1: Governance and Leadership

Strong governance and leadership structures are essential to effective decision-making, coordination, and planning for emergency communications. While the existence and growth in governance bodies is a significant accomplishment, many of these entities were originally established to address land mobile radio (LMR) interoperability issues. Evolving technology and rising expectations in emergency communications change the traditional roles and responsibilities within the public safety community, requiring strong, broader scopes and unified governing bodies. Fortunately, there is already a strong foundation for future progress. State, local, tribal, and territorial governments should focus on formalizing, expanding, and updating current structures, processes, and investments in governance and leadership.

In FY 2020, grant recipients are encouraged to invest in emergency communications governance and leadership structures for coordinating statewide and regional initiatives that reflect the evolving emergency communications environment.<sup>9</sup> These investments are critical for assessing needs, conducting statewide planning, coordinating investments, ensuring projects support the SCIP, maintaining and improving communications systems, and planning for future communications improvements. Formal governance and leadership structures can also facilitate the development of operating procedures and planning mechanisms that establish priorities, objectives, strategies, and tactics during response operations.<sup>10</sup>

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

---

<sup>9</sup> See the *Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials* at: <http://www.dhs.gov/safecom/governance>.

<sup>10</sup> See the *National Incident Management System Implementation Objectives* at: <http://www.fema.gov/national-incident-management-system>.

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

- Develop/sustain the SIGB or SIEC activities and SWIC position
  - In accordance with DHS/FEMA requirements, all states and territories receiving Homeland Security Grant Program funds are required to designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government, to include establishing statewide plans, policies, and procedures, and coordinating decisions on communications investments
- Formalize and adapt governance structures and processes to address the evolving operating environment, including:
  - Include and coordinate with emergency communications leaders (e.g., 911 leaders, IPAWS Program Management Office, RECCWGs, utilities commissions) and representatives from multiple agencies, jurisdictions, disciplines, levels of government, tribes, rural areas, subject matter experts, and private industry when developing strategic and operational plans and policies, and during training and exercises
  - Identify and include information management, network infrastructure, and cybersecurity representatives in governance membership or through formalized coordination to undertake technology integration and migration initiatives (e.g., broadband, 911, alerts and warnings, information management, network infrastructure, cybersecurity), as well as identify and address legislative and regulatory issues associated with emerging technology
  - Review and update key operating documents for SIGB or SIEC (e.g., charters, agreements, policies, procedures) to ensure they are positioned to address new technology deployments and facilitate coordination with the SWIC
  - Formalize and regularly review cross-jurisdictional, multi-state, or multi-organizational agreements (e.g., memoranda of understanding [MOU], mutual aid agreements) to account for changes to resources, capabilities, and information- or technology-sharing needs
  - Integrate emergency communications governance and leadership into broader statewide planning efforts (e.g., FirstNet deployment and radio access network buildout, 911 system migration, IT enhancements) to ensure emergency communications needs are represented
  - Increase regional structures or processes to foster multi-state coordination and information sharing
  - Conduct outreach and education to continually assess and address user needs
  - Develop governance to aid in coordination of messaging within partnering IPAWS Alerting Authorities; improve the common operating picture; and create awareness of existing plans, policies, and procedures

**2.2 Priority 2: Planning and Procedures**

The emergency communications community benefits from a comprehensive and inclusive approach to planning. The NECP recommends that response agencies seek to improve responders' ability to communicate and share information with others through formal, written strategies, plans, and standard operating procedures (SOPs) that integrate the capabilities of all users and account for the entire system lifecycle. Through development and updating of their SCIPs, states, tribes, and territories engage multiple jurisdictions, disciplines, and levels of government in planning, incorporating all emergency communications needs. The SCIP serves as the primary strategic plan for emergency communications, while other plans outline specific operational coordination or tactical procedures, including Tactical Interoperable Communications Plans (TICPs) and FEMA Regional Emergency Communications Plans (RECPs). TICPs are designed to allow urban areas, counties, regions, states/territories, tribes, or federal agencies to document interoperable communications governance structures, technology assets, and usage policies and procedures. RECPs, along with their associated state, territorial, or tribal annexes, serve to 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. Updating plans and SOPs to address emergency communications gaps, new technologies, and stakeholder needs helps to improve emergency communications and response across the whole community. This continuous and comprehensive planning enables agencies to effectively identify, prioritize, and coordinate to ensure proposed investments support statewide, tribal-wide, and territory-wide planning priorities.

In FY 2020, grant recipients should continue to target funding toward planning activities, including updates of statewide, tribal-wide, and territory-wide plans, and ensure plans incorporate the capabilities and needs of all emergency communications systems throughout their lifecycles. The goal of this priority is to ensure emergency communications needs are continually assessed and integrated into risk assessments and preparedness plans, including continuity planning efforts. These planning activities must include analyzing threats and vulnerabilities that may affect communications resilience and developing investment plans and SOPs to mitigate identified risks. Stakeholders are encouraged to target funding toward planning, stakeholder outreach, assessment of user needs, and other activities that will help to engage the whole community in emergency communications planning initiatives.

**To support this priority, grant recipients should target funding toward critical planning activities, including the following:**

- Update SCIPs, other strategic plans, and procedures to:
  - Reflect the NECP strategic goals and objectives into measurable goals, activities, and milestones
  - Incorporate whole community concepts<sup>11</sup>
  - Integrate lifecycle planning to inform agency funding decisions
  - Address capabilities (e.g., voice, video, data), findings, and gaps identified in state-level preparedness reports, risk and vulnerability assessments, and After-Action Reports (AAR) from real-world incidents and planned exercises
  - Identify and address FCC directives affecting current or planned public safety communications systems (e.g., narrowbanding, T-Band migration, systems operating in the 700 megahertz [MHz] public safety broadband spectrum, 800 MHz rebanding)
  - Incorporate a multifaceted approach to ensure the confidentiality, integrity, reliability, and availability of data
- Support statewide emergency communications and preparedness planning efforts through allocation of funding to the following planning activities:
  - Conduct and attend planning meetings
  - Engage the whole community in emergency communications planning, response, and risk identification
  - Develop and perform risk, resiliency, and vulnerability assessments (e.g., cyber, threat and hazard identification and risk assessment [THIRA])
  - Incorporate risk management strategies for continuity and recovery
  - Integrate emergency communications assets and needs into state-level plans
  - Coordinate with SWIC, State Administrative Agency (SAA),<sup>12</sup> and state-level planners (e.g., 911 planners, utilities commissions) to ensure proposed investments align to statewide plans and comply with technical requirements

---

<sup>11</sup> Per the *National Preparedness Goal*, whole community is formally defined as, “A focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of federal, state, and local governmental partners in order to foster better coordination and working relationships.”

<sup>12</sup> Many federal grants are awarded to a designated SAA as the official recipient and administrator for the grant, responsible for sub-recipient oversight of grant-funded activities.

- o Establish a cybersecurity response plan including continuity of vulnerable communications components, such as Radio Frequency (RF)-based communications that do not rely on public infrastructure
- Identify, review, establish, and improve SOPs in coordination with response agencies at all levels of government to:
  - o Ensure federal, state, local, tribal, and territorial roles and responsibilities are clearly defined
  - o Ensure communications assets and capabilities are integrated, deployed, and utilized to maximize interoperability
  - o Address threats, mitigate vulnerabilities, and identify contingencies for the continuity of critical communications

### **2.3 Priority 3: Training, Exercises, and Evaluation**

NECP Goal Demonstrations, AARs, and similar assessments reveal that jurisdictions are better able to respond to emergencies due in part to regular training and exercises. Training, exercises, and evaluations help response personnel understand their communications roles and responsibilities during an emergency, as well as processes for working with other agencies. Further, as communications technologies continue to evolve, the need for training and exercises becomes even greater to ensure personnel are proficient in using existing and new technologies. The NECP recommends agencies involve responders from all levels of government, as well as non-governmental stakeholders, to practice a whole community response. It also recommends agencies utilize all types of communication technologies, and identify gaps and problems with technologies or protocols.

In FY 2020, grant recipients should continue to invest in communications-related training, exercises, and evaluations to address gaps identified in response and recovery operations, which should include thoroughly testing resiliency and continuity of communications. Grant recipients are encouraged to participate in training and exercises across all levels of government and with other entities that will better assist jurisdictions to prepare for disasters and identify, assess, and address capability gaps.

**To support this priority, grant recipients should target funding toward certified training, exercises, and evaluation activities, including:**

- Conduct *National Incident Management System* (NIMS)-compliant training (e.g., training in Incident Command System [ICS] and the ICS Communications Unit such as Communications Unit Leader [COML], Communications Technician [COMT], Radio Operator [RADO], Incident Tactical Dispatcher [INTD], Auxiliary Communications [AUXCOMM], and Incident Communication Center Manager [INCM])<sup>13</sup>
- Improve states', tribal, and territories' ability to track and share trained Communications Unit personnel during response operations (e.g., include Communications Unit training plan within statewide plans such as the SCIP)
- Conduct frequent training and exercises involving personnel from all levels of government who are assigned to operate communications capabilities, to test communications systems and personnel (e.g., include emerging technologies and system failure), and utilize third-party evaluators with communications expertise
- Incorporate human factors in training and exercises to address the demands that voice, video, and data information place on personnel, to ensure that responders effectively use and are not overloaded by available information
- Perform exercises that support and demonstrate the adoption, implementation, and use of the NIMS concepts and principles

---

<sup>13</sup> Regular training on NIMS/ICS concepts is needed to ensure new and existing staff are proficient in NIMS/ICS concepts. For NIMS-compliant training, see: <https://www.fema.gov/nims-training>.

- Hold cross-training and state, regional, or national level exercises to validate plans and procedures to include tribes, nongovernmental organizations, and public sector communications stakeholders
- Provide training and exercises on new and existing systems, equipment, and SOPs
- Develop or update training and exercise programs to address new technologies, data interoperability, cybersecurity, use of federal and national interoperability channels, personally identifiable information, and continuity of communications
- Test communications survivability, resilience, and continuity of communications, to include validation of continuity procedures and operational testing of backup systems and equipment
- Develop and support instructor cadres to expand training for communications-support personnel
- Assess and update training curriculums and exercise criteria to reflect changes in the operating environment and plain language protocols
- Identify opportunities to integrate private and public sector communications stakeholders into training and exercises, as well as cost-effective approaches (e.g., distance learning)
- Offer cyber training and education on the proper use and security of devices and applications, phishing, malware, other potential threats, and how to guard against attacks
- Provide regular training and exercises for alerting authorities incorporating the use of IPAWS

#### **2.4 Priority 4: Activities that Enhance Communications Coordination**

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

In FY 2020, grant recipients are encouraged to update inventories of communications assets and share information within their state, tribe, or territory and region (e.g., neighboring states, tribes, or territories) that are most likely to request support during emergencies or events. This can be achieved by working with SWICs to update inputs to the Communication Assets Survey and Mapping (CASM) Tool—a web-based tool that assists public safety agencies to collect and visualize data, and assess inter-agency interoperability based on communications assets and interoperability methods.<sup>14</sup> Grant applicants and recipients should identify gaps in capabilities and target funding toward those gaps. In addition, grant recipients must continue to implement NIMS ICS principles during all incidents and planned events. Grant applicants and recipients are also encouraged to actively engage neighboring jurisdictions—both internal and external to the state, local, tribe, or territory—to coordinate response planning and seek mutual aid agreements for large-scale responses. Agencies should also collaborate and encourage alerting practices between levels of government including installing resilient communications to coordinate the distribution of alerts.

---

<sup>14</sup> CISA hosts Public Safety Software Tools on the SAFECOM website at: <https://www.dhs.gov/safecom/public-safety-software-tools>. Tools include the CASM Resource Finder, the electronic National Interoperability Field Operations Guide (eNIFOG), and electronic Auxiliary Communications Field Operations Guide (eAUXFOG) mobile applications. Users may request online training from CISA Technical Assistance at: <https://www.cisa.gov/ictapscip-resources>.

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

- Promote projects that confirm implementation of NIMS, the continued use of ICS and information sharing:
  - Establish or enhance primary, secondary, and backup communications capabilities and share appropriate ICS forms and information illustrating the status of an agency's capabilities
  - Assess and improve the timeliness of notification, activation, and response of communications systems providers to support the Incident Commander and Incident Management Team(s) requirements at incidents and planned events
- Enhance the coordination and effective usage of communications resources
  - Ensure inventories of emergency communications resources are updated and comprehensive, and readily share information about features, functionality, and capabilities of operable and interoperable communication resources with partners
  - Promote assessment of communications assets, asset coordination, and resource sharing
  - Implement projects that promote regional, intra- and inter-state collaboration
  - Support initiatives that engage the whole community, including commercial and non-traditional communications partners (e.g., auxiliary communications, volunteers, utilities)
- Develop or update operational protocols and procedures
  - Develop, integrate, or implement NIMS aligned SOPs to facilitate the integration, deployment, and use of communications assets
  - Test communications capabilities and personnel proficiency through training, exercises, and real-world events and address needs identified in statewide plans, AARs, or assessments through comprehensive action plans
  - Develop recommended guidelines regarding the use of personal communications devices (e.g., bring your own device) for official duties based on applicable laws and regulations
  - Review usage of Priority Telecommunications Services (e.g., Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service) and ensure SOPs govern the programs' use, execution, and testing
  - Plan for Alerting Authorities to ensure the highest state of readiness of existing capabilities for resilient and interoperable alerts, warnings, messaging and notifications using current local, county, state, and federal systems, and when applicable, the IPAWS
  - Review uses of the NPSBN, or FirstNet, and ensure SOPs govern the programs' use, execution, and testing
- Strengthen resilience and continuity of communications
  - Inventory and typing of resources and other activities that strengthen resilience and provide backup communications solutions (e.g., radio caches, Cell on Wheels)
  - Establish testing and usage observations of primary, secondary, and backup communications
  - Address system and staffing for continuity of operations planning

**2.5 Priority 5: Standards-based Technology and Infrastructure**

Public safety agencies continue to maintain and evolve LMR infrastructure for mission critical voice capabilities, including the pursuit of shared Project 25 (P25) radio systems and infrastructure. With acknowledgement of the need for enhanced data capabilities, many public safety organizations are also preparing to implement broadband solutions. In addition, Next Generation 911 (NG911) systems are being deployed. The public safety community continues to develop strategies and technology roadmaps for implementing standards-based, vendor-neutral devices and applications that can sustain the unique public safety operating environment and provide mission critical communications.

In FY 2020, grant recipients should continue to invest in infrastructure that is standards-based to enable interoperability between agencies and jurisdictions, regardless of vendor. Grant recipients should include technical specifications in procurement agreements with vendors and obtain sufficient documentation to verify infrastructure is compliant to applicable standards. Grant recipients are strongly encouraged to invest in equipment that will sustain and maintain current LMR capabilities while planning for new technologies and capabilities that may not have fully defined standards. As emergency communications capabilities continue to evolve, recipients should participate in community outreach and planning to ensure new capabilities are interoperable and all user requirements are incorporated.

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

- Sustain and maintain current LMR capabilities
- Purchase and use P25 compliant LMR equipment (see P25 Compliance Assessment Program [CAP] approved equipment list) for mission critical voice communications<sup>15</sup>
- Support rapid and far-ranging deployment of the NPSBN and use of FirstNet devices and applications dedicated for public safety using multi-layered, proven cybersecurity and network security solutions<sup>16</sup>
- Transition towards NG911 capabilities in compliance with NG911 standards
- Support standards that allow for alerts, warnings, and notifications across different systems
- Secure and protect equipment, information, and capabilities from physical and virtual threats
- Acquire, sustain, and maintain Common Alerting Protocol compliant software that meets IPAWS system requirements
- Employ standards-based information exchange models and data sharing solutions
- Sustain and ensure critical communication systems connectivity and resiliency, including backup solutions, among key government leadership, internal elements, other supporting organizations, and the public under all conditions
- Support standards and practices that enhance survivability and resilience to electromagnetic effects
- Ensure all communications systems and networks are traced from end-to-end to identify all Single Points of Failure, including redundancy at critical infrastructure facilities, and:
  - Sustain availability of backup systems (e.g., backup power, portable repeaters, satellite phones, High Frequency [HF] radios)
  - Ensure diversity of network element components and routing
  - Plan for geographic separation of primary and alternate transmission media
  - Maintain spares for designated critical communication systems
  - Work with commercial suppliers to remediate Single Points of Failure
  - Maintain communications capabilities to ensure their readiness when needed

---

<sup>15</sup> For more information on P25 requirements, see: <http://www.project25.org/>. For a list of P25 CAP approved equipment, see: <https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment>.

<sup>16</sup> Applicants interested in broadband investments should consult with the FirstNet Authority to ensure investments meet all technical requirements to operate on the network. Please refer to the Authority's contact information at: <https://firstnet.gov/>.

## 2.6 Priority 6: Cybersecurity

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

In FY 2020, grant recipients should invest in solutions that enhance cybersecurity posture. Cybersecurity must be addressed through planning, governance, and technology solutions that secure networks. Recipients should ensure cybersecurity planning is comprehensive and maintained throughout the lifecycle of all network components. Cybersecurity risk management should also include updates to non-technology support activities, such as mutual aid agreements, SOPs, and policy development. Personnel should be trained on the latest security, resiliency, continuity and operational practices and maintain in-service training as new technology and methods are made available.

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

- Develop and maintain cybersecurity risk management
- Implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity*<sup>17</sup> (Cybersecurity Framework) to complement an existing risk management process or to develop a credible program if one does not exist. The NIST Cybersecurity Framework establishes five functions to integrate cybersecurity into mission functions and operations, including:
  - Identify, evaluate, and prioritize risks
  - Protect against identified risks
  - Detect risks to the network as they arise
  - Deploy response capabilities to mitigate risks
  - Establish recovery protocols to ensure the resiliency and continuity of communications
- Perform a Cyber Resilience Review<sup>18</sup>
- Identify and implement standards for cybersecurity that fit system and mission needs while maintaining operability and interoperability
- Develop incident response plans, recovery plans, resiliency plans, and continuity of operations plans in anticipation of physical or cybersecurity incidents
- Mitigate cybersecurity vulnerabilities with consideration of potential impacts of cybersecurity risk management on interoperability with the broader community
- Identify and mitigate equipment and protocol vulnerabilities

---

<sup>17</sup> NIST released the *Framework for Improving Critical Infrastructure Cybersecurity*, which is a voluntary risk-based approach to cybersecurity that uses industry guidelines to help organizations manage cyber risks to critical infrastructure. For more information, see: <https://www.nist.gov/cyberframework>.

<sup>18</sup> CISA helps organizations use the NIST Cybersecurity Framework to improve cyber resilience. For more information, see: <https://www.us-cert.gov/resources/cybersecurity-framework>.

### **3. Before Applying**

---

Before applying for federal funds for emergency communications, applicants should:

- Review the NECP and SCIP
- Coordinate with statewide emergency communications leaders
- Recognize changes in the emergency communications ecosystem
- Understand federal grant requirements and restrictions

#### **3.1 Review the NECP and SCIP**

Grant applicants should read the NECP to understand the national emergency communications strategy, and to ensure proposed projects support national goals and objectives. Similarly, grant recipients should review their state or territory's SCIP to ensure proposals support statewide plans to improve communications across all emergency communications systems and capabilities. Some federal grants (e.g., Homeland Security Grant Program) require applicants to align project activities to their SCIP, so it is a best practice for all applicants to describe how proposed projects align to the needs identified in their strategic plans and performance measures.

#### **3.2 Coordinate with Statewide Emergency Communications Leaders**

To ensure projects are compatible, interoperable, and support statewide plans and strategies, grant applicants should consult the appropriate statewide leaders or entities prior to developing projects for funding. Some federal programs require or encourage coordination of grant submissions with the SWIC and other statewide leaders (e.g., Emergency Management Agency Director, 911 Administrator, Homeland Security Director), as well as require applicants to attach a letter of project support from these leaders. Grant applicants should also consult the SIGB or SIEC, as they serve as the primary steering group for the statewide interoperability strategy. Additionally, grant recipients should consult any subject matter experts serving on governance bodies such as broadband experts, chief information officers, representatives from utilities, or legal and financial experts when developing proposals.

#### **3.3 Recognize Changes in the Emergency Communications Ecosystem**

Grant recipients should understand the more complex and interdependent ecosystem that has emerged due to evolving technologies, risks, stakeholders, and policies impacting many facets of emergency communications including planning, operations, equipment, and training. Key issues impacting federal emergency communications grants include developments in advanced technologies, national policies and laws, spectrum issues, and the reduction and streamlining of grant programs.

##### ***Developments in Advanced Technologies<sup>19</sup>***

Traditionally, LMR systems were the primary capabilities the public safety community used to achieve mission critical voice communications in the field. To augment their LMR capabilities, emergency response agencies are increasingly using commercial wireless broadband services and, in some cases, procuring dedicated broadband networks for mission critical data communications. Internet Protocol (IP)-enabled networks stand to transform how public officials will communicate by providing unparalleled

---

<sup>19</sup> The term “advanced technologies” includes, but is not limited to, the use of emerging technologies to provide advanced interoperability solutions; solutions that allow the use of commercial services, where appropriate, to support interoperable communications; IP-based technologies; use of common advanced encryption options that allow for secure and vital transmissions; use of standards-based technologies to provide voice and data services that meet wireless public safety service quality; solutions that have an open interface to enable the efficient transfer of voice, data, and video signals, such as NG911 and Bridging System Interface.

connectivity and bandwidth that enhance situational awareness and information sharing. Communication network modernization is also occurring with the migration of the Nation's 911 infrastructure to NG911, an IP-based model that will enable increased resilience and redundancy in call routing, as well as the transmission of both voice and data (e.g., texts, images, geospatial location, video) to flow seamlessly from the public, through the 911 network and eventually, directly to first responders. Also, the deployment of a nationwide public alerting system is using traditional media, such as broadcast and cable, as well as IP-based technologies to transmit alerts to mobile phones and other devices.

Public safety IT systems include sensitive data, such as law enforcement information and electronic medical records, which create new security considerations including storage, access, and authentication. While electronic access to this data enables more effective response operations, it also poses risks including system failures, lack of user or server connection, and hostile hackers. As the community adopts new technologies and applications, then it too must increase understanding and planning for the security risks associated with the open architecture and vast complexity of IP-based technologies and services.

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

The convergence of technologies and risks in this evolving ecosystem shows the importance of ongoing planning for emergency communications. Grant recipients and their respective governance and leadership must consider all components that support LMR, broadband, cyber, and IP-based technologies as they update strategic plans and common operational protocols that ensure the operability, interoperability, and continuity of emergency communications systems. Additionally, grant recipients should prioritize maintaining LMR systems and other emergency communications capabilities gained in recent years as they gradually adopt and deploy IP-based technologies and services.

### **National Policies and Laws**

In addition to technological developments, the Nation is evolving its approach to preparing for and responding to incidents through the *National Preparedness Goal*, which promotes a shared responsibility across all levels of government, private and nonprofit sectors, and the general public. Applicable plans, laws, and policies include the NECP, the Middle Class Tax Relief and Job Creation Act of 2012 (Public Law 112-96; 47 U.S.C. 1401), the IPAWS Modernization Act of 2015, and the Presidential Policy Directive (PPD)-8:

- **National Emergency Communications Plan.** Updated in September 2019, the focus of this Plan is to ensure strategies, resource decisions, and investments for emergency communications keep pace with the evolving environment, and the emergency response community is collectively driving toward a common end-state for communications. The NECP provides information and guidance to those that plan for, coordinate, invest in, and use communications to support response and recovery operations.<sup>20</sup>

Grant recipients should read the NECP to understand the national emergency communications strategy, and to ensure proposed investments support the goals, objectives, and recommendations of the Plan. In addition, grant applicants are encouraged to review NECP supplemental materials such as assessments, annual progress reports, and implementation documents. Additionally, grant

---

<sup>20</sup> For more information on the NECP, see: <https://www.cisa.gov/ncp>.

applicants should work with the SWIC to ensure alignment of the SCIP and other emergency communications plans to the NECP.

- ***Middle Class Tax Relief and Job Creation Act of 2012.*** Signed into law on February 22, 2012, the Act established the FirstNet Authority, an independent authority within NTIA, and directed it to ensure the establishment of the NPSBN.<sup>21</sup> The Act reallocated and designated 700 MHz D Block spectrum for public safety use to the FirstNet Authority.<sup>22</sup> The Authority engaged in comprehensive outreach and consultation with public safety entities in federal, state, local, tribal, and territory jurisdictions to plan for the network. The Authority actively sought input from federal, tribal, state, and territorial governments; paid and volunteer first responders and other public safety personnel; industry; and other stakeholders on what the network should offer, how it should function, and how to meet the technical objectives of the network. The resulting FirstNet network solution is based on a single, national network architecture that evolves with technological advances and consists of a physically separate evolved packet core (EPC) network and radio access networks (RANs).<sup>23</sup>

FirstNet competes as a services-based business where eligible users choose to subscribe to a level of service that aligns with their mission needs. The principle responsibilities of federal, state, local, tribal, and territorial public safety entities are the acquisition of authorized and compatible devices and applications that operate on the network and determination of connectivity of proprietary databases that could support public safety operations. Infrastructure and maintenance costs of the network EPC, RANs, and NPSBN assets (e.g., Cell on Wheels, Cell on Light Trucks [COLTs], Satellite COLTs, Flying Cell on Wings) will be borne by the FirstNet Authority and its NPSBN contractor.

Per the Act, the FirstNet Authority delivered final state plans to governors to make an opt-in/opt-out decision. All 50 states, 5 territories, and the District of Columbia opted into the FirstNet Authority-proposed deployment and will have a FirstNet Network presence consistent with their state plan.

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

Applicants interested in investing federal funds in broadband-related projects should consult with the FirstNet Authority and the federal granting agency to understand all requirements impacting broadband investments. The FirstNet Authority is the sole nationwide licensee for Band 14 spectrum and does not anticipate entering into any other spectrum agreements. Applicants should work closely with the SWIC, statewide emergency communications leaders, and the federal granting agency to ensure projects remain in compliance with programmatic and technical requirements.

In addition to the duties of the FirstNet Authority, the Act also charged NTIA with establishing a grant program, the State and Local Implementation Grant Program (SLIGP), to assist state, regional, tribal, and local jurisdictions with planning activities to support the implementation of the NPSBN. As required by the Act, NTIA consulted with the FirstNet Authority in establishing the programmatic requirements for SLIGP. NTIA awarded \$116.5 million in grant funds to 54 state and

---

<sup>21</sup> For more information on the Act, see: <https://www.ntia.doc.gov/category/public-safety>.

<sup>22</sup> 47 U.S.C. § 1421(a).

<sup>23</sup> For more information on the FirstNet Core, see:

[http://about.att.com/story/nationwide\\_launch\\_of\\_firstnet\\_dedicated\\_core\\_network.html](http://about.att.com/story/nationwide_launch_of_firstnet_dedicated_core_network.html).

territorial recipients between July 2013 and June 2014. The first round of grants (SLIGP 1.0) expired February 28, 2018. Many recipients expended their grant funds at a lower rate of spending than NTIA anticipated. NTIA used the unspent funds from SLIGP 1.0 to award a new grant program, SLIGP 2.0, in March 2018. SLIGP 2.0 grants, totaling \$33.3 million, were awarded to 46 states and territories for planning activities to support implementation of the NPSBN. The original SLIGP period of performance had the grant awards end February 29, 2020, but all grants received a no-cost extension to extend the awards to the end by March 31, 2021, at the latest.

Additionally, the Act provides the NHTSA and NTIA with \$115 million for grants to improve 911 services. In August 2019, the agencies awarded 36 grants to states and two tribal grant recipients totaling \$109,250,000. The period of performance for the grant program ends on March 31, 2022. Grant applicants should continue to monitor current federal actions affecting broadband and 911 programs funded through the Act.<sup>24</sup>

- **IPAWS Modernization Act of 2015.** Signed into law in April 2016, Public Law 114-143 calls for the modernization of IPAWS to ensure that under all conditions, the President, federal agencies, and state, local, and tribal governments can alert and warn the civilian population in areas endangered by natural disasters, acts of terrorism, and other man-made disasters or threats to public safety.

The Modernization Act requires IPAWS to be designed to adapt to and incorporate future technologies for communicating directly with the public, provide alerts to the largest portion of the affected population feasible, and improve the ability of remote areas to receive alerts; promote local and regional public and private partnerships to enhance community preparedness and response; provide redundant alert mechanisms; and protect individual privacy.<sup>25</sup>

Additionally, the Modernization Act established the IPAWS Subcommittee to develop and submit recommendations for the National Advisory Council (NAC). The NAC provided a report to the FEMA Administrator in February 2019. The FEMA Administrator's Response to the NAC was signed in September 2019, prioritizing recommendations, highlighting what is currently planned, and identified areas where more resources are required.

- **Presidential Policy Directive–8, National Preparedness.** Signed by the President in March 2011, this directive is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation. It consists of four main components: *National Preparedness Goal*; National Preparedness System; *National Preparedness Report*; and the Campaign to Build and Sustain Preparedness. The directive emphasizes national preparedness is the shared responsibility of the whole community.<sup>26</sup> As a result, many grants that fund emergency communications now require grant applicants to engage the whole community in planning. FY 2020 federal grant programs require applicants to demonstrate how a whole community approach to project planning was used, and explain how core capabilities were improved. Applicants are encouraged to engage their community early in project development to ensure they can provide evidence of community involvement in applications, which in turn improves preparedness and response.

---

<sup>24</sup> For more information on the 911 Grant Program, visit: [http://www.911.gov/project\\_911grantprogram.html](http://www.911.gov/project_911grantprogram.html).

<sup>25</sup> For more information on the IPAWS Modernization Act of 2015, see: <https://www.congress.gov/bill/114th-congress/senate-bill/1180>.

<sup>26</sup> For more information on PPD-8, see: <http://www.dhs.gov/presidential-policy-directive-8-national-preparedness>.

### ***Spectrum Issues***

The FCC authorizes state, local, and some tribal public safety entities to use specific spectrum bands to operate emergency communications systems. By statute, the FirstNet Authority holds the FCC license for the 700 MHz public safety broadband spectrum to deploy the NPSBN. Grant applicants seeking federal funds for emergency communications projects should be aware of initiatives and actions affecting spectrum use for public safety entities. Applicants should review the following spectrum issues, confirm their proposed projects are consistent with regulatory requirements and initiatives, and consult the appropriate coordinator (e.g., Frequency Coordinator, SWIC), the FCC, and/or the FirstNet Authority early in the project development process to determine whether the grant applicant will have authority to operate in the desired spectrum, once complete. Key spectrum-related issues are described below:

- **Ultra-High Frequency (UHF)/Very High Frequency (VHF) Narrowbanding.**<sup>27</sup> The FCC mandated all non-federal LMR licensees operating between 150 and 512 MHz and using 25 kilohertz (kHz) bandwidth voice channels migrate to 12.5 kHz bandwidth or equivalent efficiency by January 1, 2013. Grant applicants should ensure existing LMR systems are compliant with these narrowbanding requirements and consult with the SWIC and the FCC on any non-compliance issues to avoid admonishment, monetary fines, or loss of license. Grant applicants that have not complied with the FCC narrowband mandate may face limitations on their eligibility for federal funding.<sup>28</sup>
- **800 MHz Reconfiguration (Rebanding).**<sup>29</sup> In 2004, the FCC ordered the reconfiguration of portions of the 800 MHz band to separate public safety systems from commercial cellular networks and thereby reduce harmful interferences. 800 MHz rebanding is complete in most areas of the U.S. but remains to be completed in the U.S.-Mexico border region. Public safety entities contemplating communication projects in areas still undergoing rebanding should consult their SWIC, the FCC, and the 800 MHz Transition Administrator, which is responsible for overseeing the rebanding process and providing technical assistance to affected licensees.
- **T-Band Migration.** The Middle Class Tax Relief and Job Creation Act of 2012 authorized the future auction of the 470–512 MHz ultra-high frequency band, referred to as the T-Band. Several large urban areas use the T-Band for public safety communications.<sup>30</sup> The Act requires the FCC to commence the auction process by 2021 and requires T-Band public safety licensees to relocate from the T-Band to other, unspecified spectrum, two years after the completion of the auction of this spectrum. The Act charges NTIA with administration of a grant program for relocation out of auction proceeds. T-Band licensees are currently eligible to relocate to public safety channels in the VHF (150-174 MHz), UHF (450-470 MHz), 700 MHz, and 800 MHz bands, to the extent channels in these bands are available, and the Commission has prioritized availability of certain channels in these bands for T-Band licensees. Spectrum may also be available through leasing, or partitioning/ disaggregation of other narrowband public safety or commercial spectrum. Grant applicants seeking funding for relocation of T-Band systems should consult the FCC,<sup>31</sup> SWIC, and

---

<sup>27</sup> For more information on narrowbanding, see: <https://www.fcc.gov/narrowbanding-overview>.

<sup>28</sup> See “Guidance for licensees for FCC’s narrowband operation requirement” at:

<https://www.fcc.gov/document/guidance-licensees-fccs-narrowband-operation-requirement>. Grant applicants with questions on narrowbanding may contact the FCC at: [narrowbanding@fcc.gov](mailto:narrowbanding@fcc.gov).

<sup>29</sup> For more information on 800 MHz reconfiguration, see: <http://www.800ta.org/>.

<sup>30</sup> T-Band markets include: Boston (MA), Chicago (IL), Dallas/Ft. Worth (TX), Houston (TX), Los Angeles (CA), Miami (FL), New York City (NY), Philadelphia (PA), Pittsburgh (PA), San Francisco/Oakland (CA), Washington DC/Maryland/Virginia.

<sup>31</sup> Grant applicants can contact the FCC Public Safety and Homeland Security Bureau at: [pshsinfo@fcc.gov](mailto:pshsinfo@fcc.gov).

a frequency coordinator<sup>32</sup> early in the project development process to ensure the project supports statewide plans for improving emergency communications, and is planned in the appropriate spectrum.

- **700 MHz Public Safety Broadband Spectrum.**<sup>33</sup> The Middle Class Tax Relief and Job Creation Act of 2012 authorized the establishment of the NPSBN, dedicated 20 MHz of spectrum (Band 14) for this purpose, and made the FirstNet Authority the single licensee for Band 14.

In general, grant applicants should consult with the regulatory agency and appropriate state-level points of contact when developing public safety projects to ensure entities are in compliance with federal spectrum initiatives and regulations, and projects will have authority to operate in the designated spectrum.<sup>34</sup> To assist state, local, tribal, and territorial levels of government, many grants that fund interoperable communications equipment allow grant funds to be used for spectrum-related activities,<sup>35</sup> including:

- Identification, assessment, coordination, and licensing of new spectrum resources
- Development and execution of spectrum migration plans
- Assessment of current communications assets, services, and capabilities
- Training associated with systems migration to new spectrum allocations
- Replacement of non-compliant communications equipment and services
- Acquiring/upgrading tower sites and facilities needed to comply with spectrum migration<sup>36</sup>
- Reprogramming existing equipment to comply with spectrum migration

### ***Reduction and Streamlining of Grants***

The elimination and consolidation of grants funding emergency communications over the past several years have increased competition for funding and necessitated increased planning among jurisdictions and disciplines. Emergency communications leaders and agencies are strongly encouraged to work with other jurisdictions and disciplines to coordinate resources and projects and to avoid duplication of activities. Additionally, when developing funding proposals, grant applicants are advised to work with state-level planning offices to incorporate emergency communications needs into statewide plans and to ensure communications projects are prioritized by states and territories. Applicants are encouraged to:

- Coordinate projects with the SWIC, neighboring jurisdictions, and multiple agencies
- Develop regional, multi-jurisdictional, multi-disciplinary, and cross-border projects to not only promote greater interoperability across agencies, but also to pool grant resources, facilitate asset-sharing, and eliminate duplicate purchases<sup>37</sup>

---

<sup>32</sup> For more information on frequency coordinators, see: <https://www.fcc.gov/general/public-safety-frequency-coordinators>.

<sup>33</sup> The public safety broadband spectrum band is 763-768 MHz and 793-798 MHz.

<sup>34</sup> Contact the FCC's Public Safety Homeland Security Bureau at [pshsinfo@fcc.gov](mailto:pshsinfo@fcc.gov) and the FirstNet Authority at [outreach@firstnet.gov](mailto:outreach@firstnet.gov).

<sup>35</sup> Generally, federal licensing fees are *not* allowable under most federal grants; however, applicants should not anticipate having such expenses as public safety entities are exempt from FCC filing fees. For more information, see: <https://www.fcc.gov/licensing-databases/fees>.

<sup>36</sup> Some federal grants do not allow construction or ground-disturbing activities. Consult the grant officer on these activities.

<sup>37</sup> Applicants should work with SWICs and the FCC to ensure projects do not interfere with the 800 MHz rebanding effort occurring along the U.S.-Canada and U.S.-Mexico borders. For more information on the rebanding process, see: <https://www.fcc.gov/general/800-mhz-spectrum>. Federal funding may not be allocated to international entities, unless authorized by law, and placement of federally-funded equipment on international property may be subject to special terms and conditions. Recipients should work closely with grant officers on these projects.

- Leverage assessment data to develop strong statements of need that can be shared with state leaders responsible for prioritizing projects for funding<sup>38</sup>
- Identify additional sources of funding for emergency communications improvements<sup>39</sup>

### **3.4 Understand Federal Grant Requirements and Restrictions**

#### **Federal Grant Requirements**

Emergency communications grants are administered by numerous federal agencies in accordance with various statutory, programmatic, and departmental requirements. Grant applicants are encouraged to carefully review grant guidance to ensure applications meet all grant requirements, including:

- Program goals
- Eligibility requirements
- Application requirements (e.g., due dates, submission dates, matching requirements)
- Allowable costs and restrictions on allowable costs
- Technical standards preferred, required, or allowed under each program, if applicable
- Reporting requirements

Additionally, recipients should be aware of common requirements for grants funding emergency communications,<sup>40</sup> including:

- **Environmental Planning and Historic Preservation (EHP) Compliance.** Recipients must comply with all applicable EHP laws, regulations, Executive Orders, and agency guidance. Recipients are strongly encouraged to discuss projects with federal grant program officers to understand EHP restrictions, requirements, and review processes prior to starting the project.
- **NIMS.** Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, requires the adoption of NIMS to strengthen and standardize preparedness response, and to receive preparedness grant funding. State, local, tribal, and territorial recipients should ensure that they meet, or are working to meet, the most recent NIMS implementation and reporting requirements as described in the applicable Notice of Funding Opportunity and NIMS Implementation Objectives published by FEMA.<sup>41</sup>
- **Stakeholder Preparedness Review (SPR) Submittal.** The Stakeholder Preparedness Review replaces the State Preparedness Report. Section 652(c) of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109-295), 6 U.S.C. §752(c), requires any state, territory, urban area, or tribe that receives federal preparedness assistance administered by DHS to submit an SPR to FEMA. The SPR is a self-assessment of a jurisdiction's current capability levels against the targets identified in the Threat and Hazard Identification and Risk Assessment (THIRA). Jurisdictions use

---

<sup>38</sup> Applicants are encouraged to use AARs and similar assessments to demonstrate where there are gaps in emergency communications, and to appeal to state-level leaders for funding to address those gaps.

<sup>39</sup> For additional sources of funding, see the *List of Federal Financial Assistance Programs Funding for Emergency Communications* posted to the SAFECOM website at: <https://www.dhs.gov/safecom/funding>.

<sup>40</sup> While these are common requirements that affect many emergency communications grants, they may not apply to all grants; therefore, applicants should consult their grant guidance and grant officer for specific questions on grant requirements.

<sup>41</sup> The NIMS Implementation Objectives reflect the concepts and principles contained in NIMS and clarify the NIMS implementation requirements in FEMA preparedness grant Notices of Funding Opportunity. As recipients and subrecipients of federal preparedness (non-disaster) grant awards, jurisdictions and organizations must achieve, or be actively working to achieve, all of the NIMS Implementation Objectives. Additional NIMS implementation guidance can be found at: <https://www.fema.gov/implementation-guidance-and-reporting>.

the SPR to estimate their current preparedness capabilities and compare those to their THIRA results to identify gaps. They also use the SPR to identify potential approaches for addressing those capability gaps.

- **Threat and Hazard Identification and Risk Assessment.** Beginning in 2019, DHS/FEMA require Homeland Security Grant Program (State Homeland Security Program and Urban Area Security Initiative), Tribal Homeland Security Grant Program, and Emergency Management Performance Grant Program recipients to complete a THIRA report every three years (previously, a THIRA was required annually). Grant recipients are also required to submit an SPR annually. Communities use the THIRA process to better understand their risks and determine the level of capabilities needed to address those risks. Through the THIRA process, communities set goals for building and sustaining their capabilities. It results in whole community-informed capability targets and resource requirements necessary to address anticipated and unanticipated risks.<sup>42</sup>

Developing and updating an effective THIRA/SPR requires active involvement from the whole community. This can result in more complete, accurate, and actionable assessments and planning efforts. Therefore, recipients should actively engage a wide variety of stakeholders in the THIRA/SPR process. Emergency communications subject matter experts should be involved in the THIRA/SPR process and provide input as appropriate, including but not exclusive to the potential impacts of threats and hazards on emergency communications. For additional information, refer to each grant program's FY 2020 Notice of Funding Opportunity for reporting requirements, including the THIRA/SPR. Grant recipients participating in risk assessments are strongly encouraged to:

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

- **Nationwide Cybersecurity Review.** Recipients and subrecipients of FY 2020 State Homeland Security Grant Program awards are required to complete the 2020 Nationwide Cybersecurity Review, enabling agencies to benchmark and measure progress of improving their cybersecurity posture. The Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent for each recipient and subrecipient should complete the Nationwide Cybersecurity Review. If there is no CIO or CISO, the most senior cybersecurity professional should complete the assessment.
- **Authority to Operate.** In establishing requirements for the NPSBN and providing 20 MHz of the upper 700 MHz spectrum to the FirstNet Authority, Congress directed the Authority to ensure the building, operation, and maintenance of a wireless, nationwide interoperable public safety broadband network based on a single national network architecture. The Authority holds the single nationwide FCC license for the 20 MHz of combined Public Safety Broadband Spectrum (758-768 MHz and 788-798 MHz), commonly referred to as Band 14. The FirstNet Authority license also incorporates two one-MHz guard bands at 769 and 799 MHz. Subscription to the NPSBN and use of approved NPSBN devices enables prioritized access to Band 14 spectrum for public safety entities.

---

<sup>42</sup> For additional information on the THIRA process, see: <https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment>.

- **Reporting.** Federal agencies are improving how they demonstrate impact and effectiveness of federal grant programs. As a result, recipients may be required to report project-level information, performance measurement data, detailed financial reports, and progress reports. Recipients are encouraged to use existing documentation and data (e.g., SCIPs, AARs, assessments) to measure performance and demonstrate how gaps in capabilities will be/were addressed through federal grant funding. Recipients are strongly encouraged to:
  - Develop performance measures at the start of the grant
  - Include interval performance measures and milestones to gauge project progress
  - Track performance and report the impact of funds on emergency communications
  - Include metrics on improvements in interval and final grant reports

Recipients should ensure all grant requirements are met and that they can implement the project as proposed and within the grant period of performance; properly manage grant funding; fulfill grant reporting requirements; and comply with federal grant restrictions.

### ***Federal Grant Restrictions***

Recipients should be aware of common restrictions on federal grant funding and should consult the grant officer with any questions, particularly as requirements vary by program.

- **Commingling or Duplication of Funds.** Since multiple agencies are involved in communications projects, projects are often funded with multiple grant programs, creating a risk of commingling and duplication. Recipients must ensure federal funds are used for purposes that were proposed and approved, and have financial systems in place to properly manage grant funds. Recipients cannot commingle federal sources of funding. The accounting systems of all recipients and sub-recipients must ensure federal funds are not commingled with funds from other awards or federal agencies.
- **Cost Sharing/Matching Funds.** Recipients must meet all matching requirements prescribed by the grant. If matching funds are required, grant recipients must provide matching funds or in-kind goods and services that must be:
  - Allowable under the program and associated with the investment
  - Applied only to one federal grant program
  - Valued at a cost that is verifiable and reasonable
  - Contributed from non-federal sources
  - Treated as part of the grant budget
  - Documented the same way as federal funds in a formal accounting system
- **Funding and Sustaining Personnel.** In general, the use of federal grant funding to pay for staff regular time is considered personnel and may be allowable. Recipients are encouraged to refer to the applicable grant program guidance and develop a plan to sustain critical communications positions in the event federal funds are not available to support the position in future years. For more information on personnel, refer to Section 4. *Eligible Activities – Personnel*.
- **Supplanting.** Most grant funds cannot supplant (or replace) funds previously funded or budgeted for the same purpose. Most federal grants funding emergency communications restrict recipients from hiring personnel for the purposes of fulfilling traditional public safety duties or to supplant traditional public safety positions and responsibilities. Review applicable grant program guidance for specific rules on supplanting.

## 4. Eligible Activities

---

The following section details eligible emergency communications activities commonly funded by federal grants, including Personnel and the four common cost categories: Planning and Organization, Training, Exercises, and Equipment.<sup>43</sup> Grant applicants seeking to improve interoperable emergency communications are encouraged to allocate grant funding to these activities but must consult the specific grant guidance for allowable costs.

The intent of this section is to raise awareness as to the types of costs that can be covered under most federal grants funding emergency communications. However, applicants should note all activities listed in this section may not be eligible for funding under all grant programs. Applicants should read each grant guidance and related information carefully to ensure activities proposed are eligible under the program before developing or submitting applications.

### 4.1 Personnel

Many federal grants allow recipients to hire full- or part-time staff, contractor staff, or consultants to assist with emergency communications planning, training, and exercise activities.<sup>44</sup> Allocating funding toward personnel helps ensure grants and grant-funded projects are managed, state-level planning meetings are attended, emergency communications needs are represented, and plans are completed. Personnel can be hired to develop and conduct training and exercises, and to complete AARs.

#### *Eligible Personnel Costs*

- **Personnel to assist with planning.** Full- or part-time staff, contractors, or consultants may be hired to support emergency communications planning activities, including:
  - o Statewide, local, tribal, territorial, or regional interoperability coordinator(s)
  - o Project manager(s)
  - o Program director(s)
  - o Emergency communications specialists (e.g., frequency planners, radio technicians, cybersecurity)
- **Personnel to assist with training.** Full- or part-time staff, contractors, or consultants may be hired to support emergency communications training activities, including personnel who can:
  - o Assess training needs
  - o Develop training curriculum
  - o Train the trainers
  - o Train emergency responders
  - o Promote cross-training and continuous training to address changes in the workforce
  - o Ensure personnel are proficient in using existing and new technologies
  - o Develop exercises to test training
  - o Support training conferences
  - o Develop and implement a curriculum covering technical issues raised by broadband and other advanced technologies
  - o Address continuity of operations planning requirements

---

<sup>43</sup> The general cost categories for grants include: Planning, Organization, Equipment, Training, and Exercises (POETE). Some grants do not provide a category for Organizational costs, but allow organizational costs to be included under the Planning cost category. Applicants should be aware that emergency communications personnel, planning, and organizational costs are often allowable under the Planning cost category for grants.

<sup>44</sup> Typically, the use of federal grant funding to pay for staff or contractor regular time is considered personnel.

- o Serve as subject matter experts (e.g., environmental engineers, grant administrators, financial analysts, accountants, attorneys)
- **Personnel to assist with exercises.** Full- or part-time staff, contractors, or consultants may be hired to support exercises. This includes personnel that will:
  - o Assess needs
  - o Plan and conduct exercises in accordance with NIMS and the Homeland Security Exercise and Evaluation Program (HSEEP)
  - o Implement NECP goal measurements and assessments
  - o Lead After Action Conferences and prepare AARs

#### ***Additional Requirements and Recommendations for Personnel Activities***

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

- **Sustaining Grant-Funded Positions.** Recipients should ensure funding for critical communications positions is sustained after the grant period of performance has ended and core capabilities are maintained.
- **Overtime.** Some federal grants permit the use of funds for overtime related to training. These expenses are limited to additional costs that result from personnel working more than 40 hours per week as a direct result of their attendance at approved activities (e.g., emergency communications training and exercises).
- **Backfill-related Overtime.** Some federal grants allow funds to be used for backfill-related overtime. These expenses are limited to costs of personnel who work overtime to perform duties of other personnel who are temporarily assigned to grant-funded activities (e.g., to attend approved, grant-funded emergency communications training or exercises). These costs are calculated by subtracting the non-overtime compensation, including fringe benefits of the temporarily assigned personnel, from the total costs for backfilling the position. Recipients should ensure grant funds can be used for overtime and consult their grant officer to correctly calculate overtime costs.

## ***4.2 Planning and Organization***

Allocating grant funding for planning helps entities identify and prioritize needs, define capabilities, update preparedness strategies, refine communications plans, identify where resources are needed most, and deliver preparedness programs across multiple jurisdictions, disciplines, and levels of government. Grant recipients are strongly encouraged to assess needs before planning projects, and to carefully plan projects before purchasing equipment.

#### ***Eligible Planning and Organization Costs***

- **Development or enhancement of interoperable emergency communications plans.** Grant funds may be used to develop or enhance interoperable communications plans and align plans to the strategic goals, objectives, and recommendations set forth in the NECP. Examples of emergency communications plans include:
  - o Plans to implement and measure the NECP
  - o SCIPs
  - o TICPs, FEMA RECPs, or other tactical or regional communications plans
  - o Disaster emergency communications plans

- o Communications system lifecycle planning, including migration planning and use of the *2018 Emergency Communications System Lifecycle Planning Guide and Lifecycle Planning Tool*<sup>45</sup>
- o Plans for narrowband conversion and compliance
- o Plans for broadband integration with broader communications capabilities
- o Plans for 800 MHz rebanding
- o Plans for relocating existing systems operating in the T-Band
- o Stakeholder statements of need and concept of operations (CONOPS)
- o As-is and proposed enterprise architectures
- o System engineering requirements
- o Acquisition planning for the procurement of systems or equipment
- o Planning for continuity of communications, including backup solutions, if primary systems or equipment fail (e.g., contingency and strategic planning)
- o Planning for training and exercises
- o Identifying security measures for communications networks and systems
- o Planning activities for the transition of 911 to NG911 (e.g., *NG911 Self-Assessment Tool*<sup>46</sup>)

- **Engagement of federal, state, local, tribal, territorial, private, and public sector entities in planning.** Many federal grants require engagement of the whole community in planning to adequately assess and address needs, and to implement the National Preparedness System. The *National Preparedness Goal* and the National Preparedness System concepts, as described in PPD–8, recognize the development and sustainment of core capabilities are not exclusive to any single level of government or organization, but rather require combined efforts of the whole community.<sup>47</sup> As a result, the following activities are often supported through federal grants funding emergency communications:
  - o Conducting conferences and workshops to receive input on plans
  - o Meeting expenses related to planning
  - o Public education and outreach on planning
  - o Travel and supplies related to planning or coordination meetings
  - o Attending planning or educational meetings on emergency communications
- **Establishment or enhancement of interoperability governing bodies.** Strong governance structures and leadership are essential to effective decision-making, coordination, planning, and managing of emergency communications initiatives. Grant funds may be used to establish, update, or enhance statewide, regional (e.g., multi-state, multi-urban area), or local governing bodies. Eligible activities may include:
  - o Developing MOUs and Memoranda of Agreement (MOA) to facilitate participation in planning and governance activities
  - o Meeting or workshop expenses associated with receiving input on plans or supporting a funded activity
  - o Increasing participation in governing bodies through public education and outreach
  - o Travel and supplies for governing body meetings
  - o Attending planning or educational meetings on emergency communications

---

<sup>45</sup> For guidance on emergency communications system lifecycle planning, see: <https://www.dhs.gov/safecom/funding>.

<sup>46</sup> SAFECOM/NCSWIC developed a dynamic *NG911 Self-Assessment Tool* for use by state, regional, and local emergency communications centers (ECCs)/public safety answering points (PSAPs) personnel. For more information or to download this tool, see: [https://www.911.gov/project\\_ng911tool.html](https://www.911.gov/project_ng911tool.html).

<sup>47</sup> Core capabilities include Prevention, Protection, Mitigation, Response, and Recovery, and are further defined in the *National Preparedness Goal* on the FEMA website at: <https://www.fema.gov/national-preparedness-goal>.

- o Developing SOPs or templates to provide access to and use of resources
  - o Continued broadband planning and coordination efforts
  - o Ensuring coordination between traditional LMR governance programs and other decision-making offices, bodies, and individuals that oversee new technology deployments in states, territories, localities, and tribes
- **Development of emergency communications assessments and inventories.** Grant recipients are encouraged to allocate grant funding to planning activities, such as assessments of:
  - o Technology capabilities, infrastructure, and equipment (e.g., updating the CASM Tool, creating fleet maps)
  - o SOPs, coordination of interoperability channels, and regional response plans
  - o Training and exercises
  - o Narrowband compliance capabilities and system coverage analysis
  - o Cost maintenance models for equipment and usage
- **Development or enhancement of interoperable emergency communications protocols.** Funds may be used to enhance multi-jurisdictional and multi-disciplinary common planning and operational protocols, including the development or update of:
  - o SOPs, shared channels and talk groups, and the elimination of coded substitutions (i.e., developing and implementing common language protocols)
  - o Partnership agreements, MOUs, and cross-border agreements
  - o Plans to integrate SOPs across disciplines, jurisdictions, levels of government, and with private entities, as appropriate, and into mutual aid agreements
  - o Response plans to specific disaster or emergency scenarios
  - o Field guides and templates for field guides
- **Planning activities for emerging technologies.** Grant funds may be used to begin planning for the NPSBN and other advanced technologies. Activities may include:
  - o Defining user needs
  - o Updating SCIPs to incorporate high-level goals and initiatives
  - o Developing plans to optimize broadband use in support of public safety operations
  - o Continued collection of broadband usage data, use cases, and needs analyses
  - o Developing agreed-upon standards for the use of common applications to promote enhanced level of situational awareness
  - o Preliminary planning for advanced technologies (e.g., alerts and warnings, NG911)
  - o Conducting assessments of cyber risks and strategies to mitigate vulnerabilities before the deployment of IP-based networks
  - o Implementing identity, credential, and access management (ICAM) solutions to address growing data management, interoperability, and cybersecurity challenges, with consideration for federated solutions, such as the *Trustmark Framework*<sup>48</sup>
- **Use of priority service programs.** Grant funds may be used to assist priority service planning and engineering, and to facilitate participation in federal priority service programs,<sup>49</sup> including:
  - o Telecommunications Service Priority (TSP)
  - o Government Emergency Telecommunications Service (GETS)
  - o Wireless Priority Service (WPS)

---

<sup>48</sup> For more information on ICAM and the *Trustmark Framework*, see: <https://www.dhs.gov/safecom/icam-resources>.

<sup>49</sup> For more information on priority services, see: <https://www.cisa.gov/emergency-communications-division-priority-telecommunications-services>.

- **Use of notifications and alerts and warnings.** Grant funds may be used to connect with national-level mass notification alert systems, including the IPAWS,<sup>50</sup> which consists of:
  - o Emergency Alert System (EAS)
  - o Wireless Emergency Alerts (WEA)
  - o National Oceanic and Atmospheric Administration All Hazards Weather Radio/HazCollect (NWR)

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

### ***Additional Requirements and Recommendations for Planning Activities***

Additional activities in support of federal planning initiatives include updating and submitting a SPR, THIRA, and SCIP, as well as demonstrating NIMS implementation.<sup>51</sup>

## **4.3. Training**

### ***Eligible Training Costs***

Recipients are encouraged to allocate federal grant funds to support emergency communications and incident response training. Communications-specific training activities should be incorporated into statewide training and exercise plans and be reflected in SCIPs. Recipients should continue to train on LMR systems as it is necessary to ensure public safety officials can achieve mission critical voice communications. As other communications technologies become integrated into response operations, the need for training becomes even more critical to ensure response personnel are maximizing the benefits that new capabilities provide. Training projects should be consistent with the NECP priorities and address gaps identified through SCIPs, TICPs, AARs, and other assessments. Training reinforces SOPs and proper equipment use by personnel. Grant recipients are strongly encouraged to include training in projects that involve new SOPs or equipment purchase.

- **Development, delivery, attendance, and evaluation of training.**<sup>52</sup> Grant funds may be used to plan, attend, and conduct communications-specific training workshops or meetings to include costs related to planning, meeting space, and other logistics costs, facilitation, travel, and training development. Communications-specific training should focus on:
  - o Use of SOPs and other established operational protocols (e.g., common language)
  - o NIMS/ICS training
  - o COML, COMT, or ICS Communications Unit position training
  - o Use of equipment and advanced data capabilities (e.g., voice, video, text)
  - o Disaster preparedness
  - o Peer-to-peer training
  - o Regional (e.g., multi-state, multi-urban area) operations
  - o Population of CASM Tool
  - o Integration of NG911, broadband devices, and applications into public safety operations

---

<sup>50</sup> For more information on IPAWS, see: <https://www.fema.gov/ipaws-components>.

<sup>51</sup> DHS/FEMA developed a *Preparedness Grants Manual* to guide grant applicants and recipients on how to manage their grants and other resources, available at: <https://www.fema.gov/media-library/assets/documents/178291>.

<sup>52</sup> DHS training catalogs are available at: <https://www.dhs.gov/training-technical-assistance>. The federal-sponsored and state-sponsored course catalogs can be found at: <https://www.firstrespondertraining.gov>.

- o Cyber education on proper use and security of devices and applications, phishing, malware, other potential threats, and how to stay on guard against attacks
  - o Evaluation and testing of public alert and warning procedures
- **Expenses related to training.** Many federal grants allow expenses related to training, including:
  - o Travel
  - o Public education and outreach on training opportunities
  - o Supplies related to training (e.g., signs, badges, materials)

#### ***Additional Requirements and Recommendations for Training Activities***

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

- **NIMS Implementation.**<sup>53</sup> State, local, tribal, and territorial entities must adopt NIMS as a condition of many federal grants. Given that implementation of NIMS requires certain training courses, recipients may target funding towards NIMS-compliant training.
- **Completion of Communications Unit Leader Training.** CISA, in partnership with FEMA, the Office for Interoperability and Compatibility, the National Integration Center, and practitioners from across the country, developed performance and training standards for the All-Hazards COML and formulated a curriculum and comprehensive All-Hazards COML Course. Recipients should target grant funding toward this training to improve on-site communications during emergencies, as well as satisfy NIMS training requirements.

#### **4.4 Exercises**

Exercises should be used to demonstrate and validate skills learned in training, and to identify gaps in capabilities. To the extent possible, exercises should include participants from multiple jurisdictions, disciplines, and levels of government and include emergency management, emergency medical services, law enforcement, interoperability coordinators, key information technology and cybersecurity personnel, public health officials, hospital officials, officials from colleges and universities, and other disciplines and private sector entities, as appropriate. Findings from exercises can be used to update programs to address gaps in emergency communications and emerging technologies, policies, and partners. Recipients are encouraged to increase awareness and availability of emergency communications exercise opportunities across all levels of government.

#### ***Eligible Exercise Costs***

- **Design, development, execution, and evaluation of exercises.** Grant funds may be used to design, develop, conduct, and evaluate interoperable emergency communications exercises, including tabletop and functional exercises. Activities should focus on:
  - o Use of new or established operational protocols, SOPs, and equipment
  - o Regional (e.g., multi-state, multi-jurisdictional) participation
  - o Integration of broadband services, devices, and applications into public safety operations
- **Expenses related to exercises.** Many federal grants allow for expenses related to exercises, including:
  - o Meeting expenses for planning or conducting exercises

---

<sup>53</sup> NIMS is a national framework for response that requires state, local, tribal, and territorial stakeholders to adopt a national ICS, complete certified training, and integrate the framework into state and local protocols. For more information on NIMS training, see: <https://www.fema.gov/national-incident-management-system>.

- o Public education and outreach
- o Travel and supplies

#### ***Additional Requirements and Recommendations for Exercise Activities***

Recipients should target funding toward federal exercise initiatives, including participation in the communications components of the National Level Exercises and the following:

- **Management and execution of exercises in accordance with HSEEP.** The HSEEP library provides guidance for exercise design, development, conduct, and evaluation of exercises, as well as sample exercise materials.<sup>54</sup>
- **Implementation of NIMS.** HSPD-5 requires all federal departments and agencies to adopt NIMS and use it in their individual incident management programs and activities, including all preparedness grants. DHS/FEMA recipients should review NIMS implementation criteria at: <https://www.fema.gov/national-incident-management-system>, and ensure all federally-funded training and exercise activities align with NIMS standards.
- **Coordination with state-level partners.** Communications-specific exercise activities should be coordinated with the SIGB or SIEC and SWIC to facilitate participation by appropriate entities (e.g., public safety, utilities, private sector, federal agencies) and resources (e.g., deployable assets).

#### **4.5 Equipment**

Emergency management and response providers must regularly maintain communications systems and equipment to ensure effective operation, as well as upgrade their systems when appropriate. Grant recipients are strongly encouraged to invest in standards-based equipment that supports statewide plans for improving emergency communications and interoperability among systems.

#### ***Eligible Expenses***<sup>55</sup>

- **Design, construction,<sup>56</sup> implementation, enhancement, replacement, and maintenance of emergency communications systems and equipment, including:**
  - o System engineering requirements
  - o As-is and proposed enterprise architectures
  - o Interoperability verification and validation test plans
  - o System lifecycle plans
  - o Analysis and monitoring of cybersecurity risks
  - o Migration to approved, open architecture, standards-based technologies
  - o Integration of existing capabilities and advanced technologies (e.g., multi-band/multi-mode capable radio, Internet of Things devices, artificial intelligence, machine intelligence, and data science solutions)
  - o Project management costs associated with systems and equipment
  - o Procurement of technical assistance services for management, implementation, and maintenance of communications systems and equipment

---

<sup>54</sup> HSEEP resources are available at: <https://www.fema.gov/media-library/assets/documents/32326>.

<sup>55</sup> While activities listed are generally allowable for traditional LMR investments, these activities may be restricted for broadband-related investments. Applicants are strongly encouraged to consult their federal granting agency before developing broadband proposals for funding to determine if those activities are allowable under the grant.

<sup>56</sup> Not all federal grants permit construction-related activities. Consult the grant officer to determine whether construction activities are allowed. For grants that support construction-related activities, see applicable EHP requirements to select construction-related activities in this guidance.

- o Reimbursement of cellular and satellite user fees when used for backup communications
- **Use of narrowband equipment.** The FCC mandated that all non-federal public safety land mobile licensees operating between 150-512 MHz and using 25 kHz channel bandwidth in their radio systems migrate to 12.5 kHz channels by January 1, 2013. Recipients should ensure existing systems are compliant and prioritize grant funding, where allowable, toward the following:
  - o Replacing non-compliant equipment
  - o Acquiring/upgrading additional tower sites to maintain coverage after conversion
  - o Reprogramming existing equipment to operate in compliance with the FCC's rule
- **Site upgrades for emergency communications systems.**
  - o Installing or expanding battery backup, generators, or fuel systems
  - o Evaluating existing shelter space for new communications equipment
  - o Conducting tower loading analysis to determine feasibility of supporting new antennas and equipment
  - o Analyzing site power and grounding systems to determine upgrades needed for additional communications equipment
  - o Analyzing physical site security provisions for upgrades and enhancements (e.g., fences, lighting, alarms, cameras, shelter access hardening, protective measures)
  - o Evaluating Public Safety Answering Points and other 911 infrastructure sites to determine hardware and software upgrades
- **Upgrading connectivity capabilities for emergency communications systems.**
  - o Documenting existing wireline and wireless backhaul resources to determine used and excess capacity (e.g., connectivity type of either fiber, wireline, or cable at communications sites and existing public safety facilities)
  - o Analyzing existing IP backbone to determine gaps in supporting high bandwidth public safety communications system access and applications
  - o Planning and modeling network capacity to ensure backhaul links and aggregation points are appropriately provisioned
  - o Upgrading existing backbone to support advanced capabilities (e.g., multi-protocol line switching)
  - o Installing fiber optic connections and microwave connectivity to support enhanced communications and networking capabilities
  - o Assessing and documenting usage of wireless communications capabilities including:
    - Mobile data systems facilitated through government-owned or commercial services
    - Applications
    - Devices or platforms supported
    - Speed/capacity
    - Accessible data
    - Redundancy and resiliency of systems or services
    - Cost of services and systems
    - Existing gaps in capabilities, connectivity, coverage, or application support

- **Purchase of:**
  - Standards-based interoperable communications equipment listed on the Authorized Equipment List (AEL)<sup>57</sup>
  - P25 compliant radio equipment listed on the P25 CAP Approved (Grant-Eligible) Equipment List<sup>58</sup>
  - Broadband user equipment on the NIST List of Certified Devices<sup>59</sup>
  - Applications and services that meet appropriate protocols and standards for access to, use of, or compatibility with the NPSBN
  - Equipment that will facilitate the transition of existing systems from the T-Band to authorized spectrum
  - Ancillary equipment to facilitate planning and implementation of interoperable public safety grade communications systems and capabilities (e.g., radio frequency and network test equipment including handheld spectrum analyzers, cable testers)
  - Alerts and warnings software that is compliant with the Common Alerting Protocol standards, user friendly, and meets IPAWS system requirements

#### ***Additional Requirements and Recommendations for Equipment Purchases***

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

- **Assignment of full-time Statewide Interoperability Coordinator.** DHS/FEMA requires all states and territories that use Homeland Security Grant Program funds to designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government. Responsibilities include establishing and maintaining statewide plans, policies, and procedures, and coordinating decisions on communications investments funded through federal grants. SWIC status information will be maintained by CISA and verified by FEMA through programmatic monitoring activities for DHS/FEMA grant recipients.
- **Coordination with statewide emergency communications leaders.** Recipients are strongly encouraged to coordinate with the SWIC, other emergency communications governance bodies and leadership, and appropriate state, local, tribal, and territorial partners to ensure consistency with statewide plans, and compatibility among existing and proposed emergency communications systems.
- **Compliance with technical standards.** DHS/FEMA recipients must ensure all grant-funded equipment complies with technical standards in the *SAFECOM Guidance Appendix B*, unless otherwise noted in a program's grant guidance.<sup>60</sup> Other federal grants require recipients to explain how their procurements will comply with applicable standards for LMR, IP-based systems, and alert and warning systems or provide compelling reasons for using non-standards-based solutions. Recipients should document all purchases and evidence of compliance with standards-based requirements.

---

<sup>57</sup> For a list of equipment typically allowed by DHS/FEMA grants, see: <https://www.fema.gov/authorized-equipment-list>. The AEL consists of 21 equipment categories further divided into sub-categories and individual equipment items.

<sup>58</sup> For a list of P25 compliant radio equipment, see: <https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment>.

<sup>59</sup> For a list of NIST certified devices, see: <https://www.nist.gov/ctl/pscr/process-document-nist-list-certified-devices>.

<sup>60</sup> Technical standards and requirements vary among federal grant programs (especially grants funding research and testing). Applicants should review grant guidance to ensure specific standards, terms, and conditions are met.

DHS/FEMA grant recipients must adhere to compliance requirements specified in *SAFECOM Guidance Appendix D*.

- **Compliance with FCC Requirements.** Applicants are encouraged to consult with the FCC during application development to determine whether projects will be able to access the appropriate spectrum for planned operations or if a waiver is needed. Contact the FCC at [PSHSBinfo@fcc.gov](mailto:PSHSBinfo@fcc.gov).
- **Compliance with federal EHP laws and policies.** Recipients must ensure federally-funded projects comply with relevant EHP laws. Construction and installation of communications towers and other ground-disturbing activities frequently requires EHP review. Each agency (and sometimes each program) has its own EHP compliance process. Recipients should discuss proposed construction-related activities with federal granting agencies *before* beginning work to determine whether proposed activities are allowed, and to determine if proposed activities are subject to EHP review.<sup>61</sup>
- **Adoption of new technologies.** Recipients are encouraged to migrate to approved, open architecture, standards-based systems and to integrate existing and other advanced technologies, applications, and software (e.g., multi-band/multi-mode capable radio) to expand disaster communications capabilities among emergency response providers.
- **Sustainment of current LMR capabilities.** Grant recipients are strongly encouraged to sustain current LMR capabilities for mission critical voice capabilities so that systems continue to deliver reliable communications.
- **Compliance with federal procurement requirements.** As a condition of funding, recipients agree to comply with federal procurement requirements. Recipients are responsible for ensuring open and competitive procurements, subject to the specific programmatic requirements of the grant, and applicable state or local procurement requirements. Recipients are required to have written procurement policies in place, are encouraged to follow the same policies and procedures it uses for procurement from its non-federal funds, and should include any clauses required by the Federal Government. The following are key procurement tenets when using federal funds:
  - Procurement transactions should be conducted to ensure open and free competition
  - Recipients/sub-recipients may not supplant, or replace, non-federal funds that are already budgeted or funded for a project
  - Recipients/sub-recipients should avoid non-competitive practices (e.g., contractors that developed the specifications for a project should be excluded from bidding)
- **Promotion of regional capabilities.** Grant recipients should coordinate and collaborate with agencies from neighboring states and regions to facilitate regional operable and interoperable solutions, including shared solutions.
- **Development of communications system lifecycle plans.** Emergency responders must upgrade and maintain communications systems to ensure effective operation. Some programs require recipients to submit system lifecycle plans for equipment purchased with federal grant funds. As a result, recipients should develop a system lifecycle plan for any communications system.
- **Understanding of cost share.** Federal grants often require recipients to provide a percentage of total costs allocated to equipment. Federal funds cannot be matched with other federal funds, but can be matched through state, local, tribal, or territory cash and in-kind contributions. Match requirements are often waived for ancillary territories. Grant recipients should refer to the applicable grant guidance and consult the awarding agency with any questions regarding cost share requirements.

---

<sup>61</sup> To learn more about federal EHP requirements, see the Council on Environmental Quality Regulations, 40 CFR Part 1500-1508, or the U.S. Department of Energy website at: [https://energy.gov/sites/prod/files/NEPA-40CFR1500\\_1508.pdf](https://energy.gov/sites/prod/files/NEPA-40CFR1500_1508.pdf).

## 5. Emergency Communications Systems and Capabilities

---

Emergency communications are accomplished through many technologies, each with varying capabilities, standards, and features. As the public safety community adopts new technologies, LMR will remain an important tool for mission critical voice communications for emergency responders in the field for many years to come. Successful future planning requires a multi-path approach in maintaining LMR systems' operability and interoperability while planning and deploying new emergency communications technologies. As such, grant recipients should invest in sustaining LMR capabilities while also planning for new technologies.

As LMR and IP-based technologies continue to become integrated with one another, interoperability and cybersecurity become increasingly important. When procuring equipment or software for emergency communications systems, grant recipients are strongly encouraged to purchase standards-based technologies to facilitate interoperability and security among jurisdictions and disciplines at all levels of government. Table 2 provides best practices for promoting interoperability and security in several types of emergency communications capabilities. For detailed standards and resources for each system type, refer to Appendix B.

**Table 2. Best Practices when Purchasing Emergency Communications Capabilities**

Systems	Best Practices
<b>Land Mobile Radio</b>	<ul style="list-style-type: none"> <li>Review P25 technical standards for LMR and specify applicable P25 standards and specifications in the <a href="#">P25 Steering Committee Approved List of Standards</a></li> <li>Select <a href="#">P25 Compliance Assessment Program</a> (P25 CAP) approved equipment</li> <li>Obtain documented evidence of P25 CAP compliance; in the absence of testing information on the P25 Compliance Assessment Bulletins, entities should request results of applicable test procedures identified in the P25 standards list</li> <li>Ensure additional features purchased are P25 compliant (e.g., AES 256 encryption)</li> <li>Avoid non-standard features, but if necessary, ensure features are identified and understand impact on interoperability</li> <li>Provide written justification for non-compliant P25 purchases</li> </ul>
<b>Public Safety Broadband</b>	<ul style="list-style-type: none"> <li>Seek guidance from the <a href="#">FirstNet Authority</a> on how to best incorporate broadband communications into a public safety entity's communications ecosystem</li> </ul>
<b>Alerts, Warnings, and Notifications</b>	<ul style="list-style-type: none"> <li>Read the <a href="#">IPAWS Best Practices Guide</a></li> <li>Consult with <a href="#">IPAWS Program Management Office</a> for compatible alert origination software tools</li> <li>Review the IPAWS list of critical capabilities and recommended features of an alert origination software tool</li> <li>Ensure software tool compliance with Common Alerting Protocol (CAP), the <a href="#">IPAWS CAP Profile</a>, and support of a testing environment</li> <li>Complete the IPAWS Memorandum of Agreement process</li> </ul>
<b>911 Systems</b>	<ul style="list-style-type: none"> <li>Read the <a href="#">NG911 Standards Identification and Review</a> and select a Standard Development Organization's standards</li> <li>Consult with the <a href="#">National 911 Program Office</a> regarding any updated standards</li> <li>Select IP-enabled 911 open standards equipment and software</li> </ul>
<b>Data Exchange and Information Sharing Environment</b>	<ul style="list-style-type: none"> <li>Evaluate data information sharing needs and standards based on existing systems, users, and the type of information being exchanged</li> <li>Read the <a href="#">Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data eXchange Language (EDXL)</a> and <a href="#">National Information Exchange Model (NIEM)</a> resources on data messaging standards</li> <li>Read the standards, guides, and best practices provided by the Information Sharing Framework initiative</li> </ul>

## 6. Grants Management Best Practices

Proper management of grants enables recipients to effectively implement projects and access grant funds. It also can establish the entity as a trusted and capable steward of federal funding that is able to manage additional funds in the future. This section provides guidance and best practices for recipients to use throughout the grant lifecycle. Table 3 provides best practices during the four major phases of the grant:

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

**Table 3. Suggested Actions and Best Practices to Use during Grant Cycle Phases**

Phases	Suggested Actions / Best Practices
Pre-Award	<ul style="list-style-type: none"> <li>• Review and understand the NECP, SCIP, and other applicable plans</li> <li>• Coordinate with the SWIC and other key governance bodies and leadership to document needs, align projects to plans, and identify funding options<sup>62</sup></li> <li>• Work with SAA to include projects in state preparedness plans and to secure funding</li> <li>• Review program requirements included in grant guidance</li> <li>• Consult the federal granting agency, spectrum authority (i.e., FCC or FirstNet Authority), and <i>SAFECOM Guidance</i> when developing projects</li> <li>• Align projects to federal and state-level plans and initiatives</li> <li>• Include coordination efforts with the whole community in applications</li> <li>• Identify staff to manage financial reporting and programmatic compliance requirements</li> <li>• Develop project and budget milestones to ensure timely completion</li> <li>• Identify performance measures and metrics that will help demonstrate impact</li> <li>• Consider potential impacts of EHP requirements on implementation timelines</li> <li>• Ensure proper mechanisms are in place to avoid commingling and supplanting of funds</li> <li>• Evaluate the ability of sub-recipients to manage federal funding</li> <li>• Consider how the project will be sustained after grant funding has ended</li> </ul>
Award	<ul style="list-style-type: none"> <li>• Review award agreement to identify special conditions, budget modifications, restrictions on funding, pass-through and reporting requirements, and reimbursement instructions</li> <li>• Update the proposed budget to reflect changes made during review and award</li> <li>• Inform sub-recipients of the award and fulfill any pass-through requirements</li> </ul>
Post Award	<ul style="list-style-type: none"> <li>• Establish repository for grant file and related data to be collected and retained from award through closeout, including correspondences, financial and performance reports, project metrics, documentation of compliance with EHP requirements and technology standards</li> <li>• Ensure fair and competitive procurement process for all grant-funded purchases</li> <li>• Understand the process for obtaining approval for changes in scope and budget</li> <li>• Adhere to proposed timeline for project and budget milestones; document and justify any delays impacting progress or spending</li> <li>• Leverage federal resources, best practices, and technical assistance</li> <li>• Complete financial and performance reports on time</li> <li>• Draw down federal funds as planned in budget milestones or in regular intervals</li> <li>• Complete projects within grant period of performance</li> </ul>
Closeout	<ul style="list-style-type: none"> <li>• Ensure all projects are complete</li> <li>• Maintain and retain data as required by the award terms and conditions</li> <li>• File closeout reports; report on final performance</li> </ul>

<sup>62</sup> Stakeholders can also contact their respective [CISA Emergency Communications Coordinator](#) for guidance.

## **7. Funding Sources**

---

Applicants should consider all available funding sources, including traditional grants to help fund initial capital investments or improvements to communications systems, as well as other sources of funding that may partially fund emergency communications projects.

### ***Traditional Grant Funding***

CISA is charged with coordinating federal grants funding emergency communications. Through its work with the ECPG Grants Focus Group, CISA identified more than 20 federal grants and loans that fund emergency communications in FY 2019.<sup>63</sup> When applying for these funds, grant applicants are encouraged to:

- Identify current grant funding available and alternative sources of funding
- Review eligibility requirements, program goals, and allowable costs
- Understand what past grants have funded in your jurisdiction
- Partner with entities eligible to receive other funding sources

### ***Other Sources of Federal Funding***

While *SAFECOM Guidance* traditionally covered federal financial assistance programs, there are other grant and loan programs that can provide extensive funding for state, local, tribal, and territorial public safety communications needs. For example, the U.S. Department of Agriculture (USDA) Rural Utility Service integrated interoperable emergency communications and 911 upgrade authority in its Telecommunications Loan Program, and loans and grants from USDA Rural Development's Community Facilities Program provided critical funding for emergency communications projects. While loans offer an alternative to traditional grants, applicants should work with financial experts to understand loan terms and ensure their proposals meet all requirements under each program.

Also, there are several federal programs that are not solely focused on public safety communications (e.g., Rural Telecommunications and Rural Electrification Programs). These programs can improve access to 911 services; provide all hazards warnings; improve integration and interoperability of emergency communications; provide critical infrastructure protection and outage prevention; and increase the reliability of standby power to emergency responders. Applicants are encouraged to identify additional funding sources, such as rural grants and loans, and work with eligible entities for those programs to improve communications infrastructure.

---

<sup>63</sup> For an updated list of federal grants and loans that fund emergency communications, see: <https://www.dhs.gov/safecom/funding>. Applicants can find and search grants and loans at: <https://www.grants.gov>.

## ***Funding and Sustainment Resources***

CISA, SAFECOM, and NCSWIC publish numerous resources for state, local, tribal, and territorial governments and their public safety agencies to identify funding mechanisms for emergency communications projects. The following list includes educational documents and tools designed for stakeholders, available on the [SAFECOM Funding website](#).

- *Funding Mechanisms for Public Safety Communications Systems*, provides an overview of various methods of funding emergency communications systems (e.g., bonds, special tax, surcharges), and specific examples of where these methods have been used to fund state and local systems. Updates are anticipated in 2020, which will include new funding and sustainment methods and considerations for implementing in your area.
- *Emergency Communications System Lifecycle Planning Guide* and *Lifecycle Planning Tool*, provide assistance to stakeholders in their efforts to fund, plan, procure, implement, support, and maintain public safety communications systems, and eventually to replace and dispose of system components.
- *Emergency Communications Systems Value Analysis Guide* and *Brochure*, assist public safety agencies evaluate communications systems and equipment for cost effectiveness and value to its users. Materials describe common system components, including considerations and features required by public safety agencies that are unique to specific roles.
- *Interoperability Business Case: An Introduction to Ongoing Local Funding*, advises the community on the elements needed to build a strong business case for funding interoperable communications.
- Various educational documents, brochures, and action memorandum to assist stakeholders identify funding and procure radio communications systems.
  - *LMR 101, Part I: Educating Decision Makers on LMR Technologies*, includes basic information for use in educating decision-makers about the importance of LMR technologies. The paper includes simple diagrams, terminology, history, and current usage of LMR technologies by public safety agencies.
  - *LMR for Decision Makers, Part II: Educating Decision Makers on LMR Technology Issues*, provides information about emerging technologies, and the impact such technologies will have on LMR systems as they evolve. Information includes discussion of the LMR-to-LTE transition, and the need to sustain mission critical voice through such transition.
  - *LMR for Project Managers, Part III: A P25 Primer for Project Managers and Acquisition Managers*, delivers an introduction about standards-based purchasing, and an overview of the P25 standard explaining its importance to public safety interoperability.
  - *LMR Brochure*, provides stakeholders with a hand-out to give to state and local decision-makers and elected officials to explain why it is important to fund and sustain LMR.
  - *LMR Action Memorandum*, provides stakeholders with basic information they can give to state and local decision-makers and elected officials on why it is important to fund and sustain public safety radio systems.

## **Appendix A – Acronym List**

---

3GPP	Third Generation Partnership Project
AAR	After-Action Report
AEL	Authorized Equipment List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions, Inc.
BSI	Bridging Systems Interface
CAP	Common Alerting Protocol
CASM	Communication Assets Survey and Mapping
CDM	Continuous Diagnostics and Mitigation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CJIS	Criminal Justice Information Services
CEQR	Council on Environmental Quality Regulations
CNSS	Committee on National Security Systems
COLT	Cell on Light Trucks
COML	Communications Unit Leader
COMT	Communications Technician
CONOPS	Concept of Operations
COW	Cell on Wheels
CSIRT	Computer Security Incident Response Team
CSRIC	Communications Security Reliability and Interoperability Council
CSSP	Communications Sector-Specific Plan
DE	Distribution Element
DES-OFB	Data Encryption Standard-Output Feedback
DHS	Department of Homeland Security
EAS	Emergency Alert System
ECC	Emergency Communications Center
ECPC	Emergency Communications Preparedness Center
EDXL	Emergency Data eXchange Language
EHP	Environmental Planning and Historic Preservation
EO	Executive Order
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute

FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FirstNet Authority	First Responder Network Authority
FY	Fiscal Year
GETS	Government Emergency Telecommunications Service
GFIPM	Global Federated Identity and Privilege Management
GRA	Global Reference Architecture
GSMA	Groupe Speciale Mobile Association
HAVE	Hospital Availability Exchange
HF	High Frequency
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
ICO	Implementation Coordination Office
ICS	Incident Command System
IDS	Intrusion Detection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEP	Information Exchange Package
IEPD	Information Exchange Package Documentation
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPS	Intrusion Prevention
IS	Independent Study
ISE	Information Sharing Environment
ISO	International Organization for Standardization
ISSI	Inter Radio Frequency Sub-System Interface
IT	Information Technology
ITU	International Telecommunications Union
kHz	kilohertz
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MHz	Megahertz
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	National Advisory Council

NASNA	National Association of State 911 Administrators
NCCIC	National Cybersecurity and Communications Integration Center
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NENA	National Emergency Number Association
NEP	National Exercise Program
NERC	North American Electric Reliability Corporation
NG-SEC	NENA Security for NG911 Standard
NHTSA	National Highway Traffic Safety Administration
NIFOG	National Interoperability Field Operations Guide
NG911	Next Generation 911
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal/Interagency Reports
NOAA	National Oceanic and Atmospheric Administration
NOFO	Notice of Funding Opportunity
NPSBN	Nationwide Public Safety Broadband Network, or FirstNet
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OMA	Open Mobil Alliance
OIC	Office for Interoperability and Compatibility
OMB	Office of Management and Budget
P25	Project 25
P25 CAP	P25 Compliance Assessment Program
PMO	Project Management Office
POETE	Planning, Organization, Equipment, Training, and Exercises
PPD	Presidential Policy Directive
PSAP	Public Safety Answering Point
PSCR	Public Safety Communications Research
PSHSB	Public Safety & Homeland Security Bureau
PTIG	Project 25 Technology Interest Group
RAN	Radio Access Network
RECCWG	Regional Emergency Communications Coordination Working Group
RECP	Regional Emergency Communications Plans

RF	Radio Frequency
RFI	Request for Information
RM	Resource Messaging
RUS	Rural Utilities Service
SAA	State Administrative Agency
SAME	Specific Area Message Encoding
SCIP	Statewide Communication Interoperability Plan
SDO	Standard Development Organization
SIGB	Statewide Interoperability Governing Body
SIEC	State Interoperability Executive Committee
SLIGP	State and Local Implementation Grant Program
SOP	Standard Operating Procedure
SoR	Statement of Requirements
SPR	Stakeholder Preparedness Review
SWIC	Statewide Interoperability Coordinator
TDoS	Telephone Denial of Service
TFOPA	Task Force on Optimal Public Safety Answering Point Architecture
THIRA	Threat and Hazard Identification and Risk Assessment
TIA	Telecommunications Industry Association
TICP	Tactical Interoperable Communications Plan
TSP	Telecommunications Service Priority
UASI	Urban Areas Security Initiative
UHF	Ultra High Frequency
USDA	United States Department of Agriculture
URT	Unified Reporting Tool
US-CERT	U.S. Computer Emergency Readiness Team
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
W3C	World Wide Web Consortium
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Service
XML	Extensible Markup Language

## **Appendix B – Technology and Equipment Standards and Resources**

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

### ***How to Use this Appendix***

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

<b><i>System Lifecycle Planning</i></b> .....	<b><i>B-1</i></b>
<b><i>Cybersecurity</i></b> .....	<b><i>B-3</i></b>
<b><i>Continuity and Resilience</i></b> .....	<b><i>B-7</i></b>
<b><i>Land Mobile Radio</i></b> .....	<b><i>B-9</i></b>
<b><i>Public Safety Broadband</i></b> .....	<b><i>B-12</i></b>
<b><i>Alerts, Warnings, and Notifications</i></b> .....	<b><i>B-14</i></b>
<b><i>911 Systems</i></b> .....	<b><i>B-16</i></b>
<b><i>Data Exchange and Information Sharing Environment</i></b> .....	<b><i>B-18</i></b>

### **System Lifecycle Planning**

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

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

Each phase of the system lifecycle planning model—Pre-Planning; Project Planning; Request for Proposals and Acquisition; Implementation; Support, Maintenance, and Sustainment; End-of-Lifecycle Assessment and Replacement; and Disposition—includes best practices, considerations, and recommended checklists to assist public safety agencies embarking on system lifecycle planning. Specifically, the checklists are designed to be torn-out, referenced, and used by project management teams throughout the system lifecycle. Table B-1 summarizes the system lifecycle planning model phases and high-level recommendations contained in the *2018 Emergency Communications System Lifecycle Planning Guide*. Reference the guide for additional information on recommendations.

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

Planning Model	Recommendations
<b>Phase 1:</b> Pre-Planning <b>Timing:</b> 6–12 months <b>Goals:</b> Inform and secure the decision to replace, upgrade, maintain, dispose of, and/or acquire a new system	<ul style="list-style-type: none"> <li>Establish the core planning team</li> <li>Research and develop system and funding options</li> <li>Decide on the optimal and alternative solutions with funding options</li> <li>Plan for frequency needs and channel programming</li> <li>Develop a business case, presentation materials, and strategic plan</li> <li>Identify a legislative- or executive-level project champion</li> <li>Present to decision-makers and secure funding to support the initial build-out and sustain the system throughout the entire lifecycle</li> </ul>
<b>Phase 2:</b> Project Planning <b>Timing:</b> 6–18 months <b>Goals:</b> Formalize the project team; identify operational and technical requirements for system replacement and upgrade; and develop the project plan	<ul style="list-style-type: none"> <li>Consider how long the planning process can take and communicate expected timeframes to elected officials</li> <li>Collect user needs and requirements and incorporate into project plans</li> <li>Engage with communications leaders early for guidance and support (e.g., Statewide Interoperability Coordinators [SWIC], Statewide Interoperability Governing Bodies [SIGB])</li> <li>Identify strong Project Sponsors (e.g., state or local elected officials)</li> <li>Begin planning the Request for Proposals (RFP)</li> </ul>
<b>Phase 3:</b> RFP and Acquisition <b>Timing:</b> 6–12 months <b>Goals:</b> Select the appropriate procurement vehicle and procure systems and components	<ul style="list-style-type: none"> <li>Develop a written action plan</li> <li>Form the RFP team</li> <li>Develop the Statement of Work (SOW)</li> <li>Include specifications or requirements in the RFP</li> <li>Establish written evaluation criteria, well before the award</li> <li>Conduct a formal objective review process and document results</li> </ul>
<b>Phase 4:</b> Implementation <b>Timing:</b> 12–18 months <b>Goals:</b> Develop an implementation plan; install new systems; test; train users; and transition from legacy to new	<ul style="list-style-type: none"> <li>Develop the implementation plan</li> <li>Understand and document testing procedures (e.g., factory testing, staging, site installation and testing, coverage verification, testing and acceptance, cut-over, final acceptance)</li> <li>Update operational procedures and train users</li> <li>Promote new communications capabilities and benefits to the community</li> </ul>
<b>Phase 5:</b> Support, Maintenance and Sustainment <b>Timing:</b> Year(s) 1–25 <b>Goals:</b> Inventory and maintain equipment; manage budget; assess and communicate needs	<ul style="list-style-type: none"> <li>Maintain an accurate inventory of equipment (e.g., scope, database tool, inventory team, processes to compile and secure data)</li> <li>Determine and execute an ongoing maintenance and operations model</li> <li>Manage the budget when the project is conceived, directly before it is funded and after delivery</li> <li>Share communications needs with decision-makers early and continually</li> </ul>
<b>Phase 6:</b> End-of-Lifecycle Assessment and Replacement <b>Timing:</b> Years 7–25 <b>Goals:</b> Determine when to replace systems or components with solutions to best fit operational and technical needs	<ul style="list-style-type: none"> <li>Conduct ongoing assessments of current system (e.g., implement a balanced scorecard) to plan for technology maturity</li> <li>Refresh or upgrade systems, as needed, to extend the life</li> <li>Determine potential replacement solutions, with consideration to support national, state, and regional interoperability initiatives; consider early adoption of new technologies; and, adhere to widely-used technical standards</li> </ul>
<b>Phase 7:</b> Disposition <b>Timing:</b> 90 days after cut-over or transition <b>Goals:</b> Determine options and dispose of legacy systems or components	<ul style="list-style-type: none"> <li>Develop the disposition plan</li> <li>Determine options (e.g., reuse or repurpose old components, consider space availability, convey surplus equipment to partner agencies) in consideration of legal or policy limitations, and business requirements</li> <li>Brief leaders on disposition plans</li> <li>Identify lessons learned following disposition</li> </ul>

## Cybersecurity

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

Land mobile radio (LMR) has long been used by emergency first responders for mission critical communications. As technologies evolve, LMR systems are exposed to greater security risks such as jamming, eavesdropping, and denial of service. In addition, the emergency response community is deploying advanced voice, video, and data services over Internet Protocol (IP)-based networks to enhance response operations. Although these services enhance capabilities, they also introduce new and significant cyber risks that the emergency response community must address. Traditional emergency communications systems have limited means of cyber entry, but IP-based platforms enable interconnection with a wide range of public and private networks, such as wireless networks and the Internet.

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

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

### *Cybersecurity Framework*

The National Institute of Standards and Technology (NIST) developed the [\*Framework for Improving Critical Infrastructure Cybersecurity\*](#) (Cybersecurity Framework) as a flexible and voluntary risk-based approach that outlines techniques to secure critical infrastructure. Recipients are strongly encouraged to implement NIST's framework to complement an existing risk management process or to develop a credible program if one does not exist. In addition to NIST materials, [sector-specific Cybersecurity Framework guidance](#) is available from CISA.

The NIST Cybersecurity Framework establishes five functions to integrate cybersecurity into mission functions and operations, including: 1) **identify**, evaluate, and prioritize risks; 2) **protect** against identified risks; 3) **detect** risks to the network as they arise; 4) deploy **response** capabilities to mitigate risks; and 5) establish **recovery** protocols to ensure the resiliency and continuity of communications. CISA's Emergency Services Sector has developed tailored guidance specific to emergency service disciplines, including a NIST Framework implementation guide with a repeatable process to identify and prioritize cybersecurity improvements.<sup>64</sup>

<sup>64</sup> Suggested resources include the [2015 ESS Cybersecurity Framework Implementation Guidance](#) and [2014 ESS Roadmap to Secure Voice and Data Systems](#).

There is considerable cybersecurity guidance available from government, industry, and academic organizations and a multitude of standards development organizations (SDOs) that contribute to technical standards and best practices. Organizations managing critical infrastructure will continue to have unique risks—different threats, different vulnerabilities, and different risk tolerances—and how they implement the standards and guidance available will vary. There is currently no one-size-fits-all network cybersecurity solution. Table B-2 lists some of the potentially-applicable standards for cybersecurity that recipients should leverage as they identify and select the standards that fit their system and mission needs. Table B-3 lists cybersecurity resources for additional information. While these lists are not exhaustive, they include some of the more comprehensive guidance for the public safety community.

**Table B-2. Cybersecurity Standards**

Organizations	Standards
<b>Third Generation Partnership Project (3GPP) Security Standards</b>	3GPP's security working group, SA3, is continuously updating security standards associated with prevalent technologies, most notably IP Multimedia Subsystem. Specifically, the group is addressing 3GPP standards for network access security, network domain security, user domain security, application domain security, and user configuration and visibility of security is important for critical infrastructure implementations. <a href="https://www.3gpp.org">https://www.3gpp.org</a> .
<b>American National Standards Institute (ANSI) / International Society of Automation (ISA)</b>	ANSI/ISA standards focus on automation and control systems solutions. The NIST Cybersecurity Framework recommends two ANSI/ISA standards for use: ANSI/ISA-62443-2-1 (99.02.01)-2009 and ANSI/ISA-62443-3-3 (99.03.03)-2013. <a href="https://www.isa.org/templates/two-column.aspx?pageid=131422">https://www.isa.org/templates/two-column.aspx?pageid=131422</a> . Also, outputs of the Alliance for Telecommunications Industry Solutions (ATIS) Emergency Services Interconnection Forum, Next Generation Interconnection Interoperability Forum, and Wireless Technologies and Systems Committee are important to the public safety community.
<b>Criminal Justice Information Services (CJIS) Security Policy</b>	CJIS standards contain information security requirements, guidelines, and agreements reflecting the will of law enforcement agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information. <a href="https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center">https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center</a> .
<b>European Telecommunications Standards Institute (ETSI)</b>	ETSI Telecommunications & Internet converged Services & Protocols for Advanced Networks (TISPAN) has been a key standardization body in creating Next Generation Network (NGN) specifications, and their Cyber Security committee focuses entirely on privacy and security activities. Of note for emergency communications are the ETSI TS 102, 123, 182, and 282 series. <a href="http://www.etsi.org/">http://www.etsi.org/</a> .
<b>Federal Information Processing Standards (FIPS)</b>	FIPS establishes the minimum security requirements for federal information systems. <a href="https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips">https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips</a> .
<b>Health Insurance Portability and Accountability Act of 1996 (HIPAA)</b>	Legislation enacted by Congress in 1997 to streamline medical regulations, privacy considerations, and the efficiency and security of medical care. The standards/rules associated with HIPAA address some of the NIST Cybersecurity Framework functions. <a href="https://www.hhs.gov/hipaa/">https://www.hhs.gov/hipaa/</a> .
<b>International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Standards</b>	The ISO/IEC 27000 series of standards provide a foundation for information security management best practices. Of interest to emergency communication networks may be ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27002, ISO/IEC 27032, and ISO/IEC 17799. <a href="http://www.iso.org">http://www.iso.org</a> .
<b>Institute of Electrical and Electronics Engineers (IEEE)</b>	IEEE produces sector-specific security standards, as well as industry guidance. Of interest to networks may be the 802, 1363, and 1619 series, as well as C37.240-2014 IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. <a href="http://www.ieee.org">http://www.ieee.org</a> .

Organizations	Standards
<b>International Telecommunication Union (ITU)</b>	A fundamental role of ITU is to build confidence and security in the use of Information and Communication Technologies. Of note for emergency communications networks include X.800, X.805, and X.1051. <a href="http://www.itu.int/">http://www.itu.int/</a> .
<b>Internet Engineering Task Force (IETF)</b>	IETF Working Groups are the primary mechanism for development of IETF standards. IETF Working Groups currently have 598 standards regarding security mechanisms, integrity mechanisms, network layer security, transport layer security, application layer security, encryption algorithms, key management, secure messaging, etc. <a href="https://www.ietf.org/">https://www.ietf.org/</a> .
<b>National Fire Protection Association 1221</b>	A standard for the installation, maintenance, and use of emergency services communications systems, including cybersecurity considerations. <a href="http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&amp;code=1221">http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&amp;code=1221</a> .
<b>NIST Recommendations on Cybersecurity (Special Publications 800 Series)</b>	NIST's 800 series provides targeted cybersecurity guidance and are strongly encouraged to be incorporated into cybersecurity planning. <a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a> .
<b>North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Regulations</b>	Reliability standards address the security of cyber assets essential to the reliable operation of the electric grid. With emerging interconnectivity of infrastructure, the emergency communications community may also need to address these standards. <a href="http://www.nerc.com/pa/CI/Comp/Pages/default.aspx">http://www.nerc.com/pa/CI/Comp/Pages/default.aspx</a> .
<b>Telecommunications Industry Association (TIA)</b>	TIA has both Cybersecurity and Public Safety working groups. Standards of particular use for emergency communications include: TR-8, TR-30, TR-34, TR-41 TR-42 TR-45, TR-47, TR-48, TR-49, TR-50 M2M, TR-51, and TIA-102. <a href="https://www.tiaonline.org/">https://www.tiaonline.org/</a> .

Table B-3. Cybersecurity Resources

Organizations	Resources
<b>Committee on National Security Systems (CNSS)</b>	<ul style="list-style-type: none"> <li>• <a href="#">CNSS Policies</a></li> </ul>
<b>Department of Homeland Security (DHS)</b>	<ul style="list-style-type: none"> <li>• <a href="#">DHS Cybersecurity Strategy</a></li> <li>• <a href="#">CISA Cyber Resilience Review</a></li> <li>• <a href="#">CISA Insights</a></li> <li>• <a href="#">Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan</a></li> <li>• <a href="#">Continuous Diagnostics and Mitigation (CDM)</a></li> <li>• <a href="#">Cybersecurity Evaluation Tool (CSET)</a></li> <li>• <a href="#">Emergency Services Sector (ESS) Cyber Risk Assessment – 2012</a></li> <li>• <a href="#">ESS Roadmap to Secure Voice and Data Systems – 2014</a></li> <li>• <a href="#">ESS Cybersecurity Framework Implementation Guidance – 2015</a></li> <li>• <a href="#">Homeland Security Grant Program Supplemental Resource: Cyber Security Guidance</a></li> <li>• <a href="#">Information Sharing Environment (ISE) Guides and Best Practices</a></li> <li>• <a href="#">National Cyber Incident Response Plan</a></li> <li>• <a href="#">National Cybersecurity and Communications Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT)</a></li> <li>• <a href="#">National Infrastructure Coordinating Center (NICC)</a></li> <li>• <a href="#">National Infrastructure Protection Plan</a></li> <li>• <a href="#">Safeguarding and Securing Cyberspace</a></li> </ul>

Organizations	Resources
	<ul style="list-style-type: none"> <li>• <a href="#">Supplement Tool: National Protection and Programs Directorate Resources to Support Vulnerability Assessments</a></li> <li>• <a href="#">Best Practices for Encryption in Project 25 Public Safety Land Mobile Radio Systems</a></li> </ul>
<b>Department of Energy</b>	<ul style="list-style-type: none"> <li>• <a href="#">Energy Sector Cybersecurity Capability Maturity Model (C2M2) Program</a></li> </ul>
<b>Executive Orders (EO) and President Directives</b>	<ul style="list-style-type: none"> <li>• <a href="#">EO 13636: Improving Critical Infrastructure Cybersecurity</a></li> <li>• <a href="#">EO 13231: Critical Infrastructure Protection in the Information Age and EO 13286</a></li> <li>• <a href="#">EO 13618: Assignment of national Security and Emergency Preparedness Communications Functions</a></li> <li>• <a href="#">Executive Office of the President, Presidential Policy Directive 21 (PPD – 21)</a></li> <li>• <a href="#">EO 13407: Public Alert and Warning System</a></li> <li>• <a href="#">EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure</a></li> </ul>
<b>Federal Bureau of Investigation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Cyber Crime</a></li> </ul>
<b>Federal Communications Commission</b>	<ul style="list-style-type: none"> <li>• <a href="#">Communications Security, Reliability and Interoperability Council (CSRIC)</a></li> <li>• <a href="#">Task Force on Optimal PSAP Architecture (TFOPA)</a></li> <li>• <a href="#">Cyber Security Planning Guide</a></li> </ul>
<b>Federal Emergency Management Agency</b>	<ul style="list-style-type: none"> <li>• <a href="#">Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC)</a></li> <li>• <a href="#">Cybersecurity Gap Analysis, FEMA National Cyber Resilient Architecture, and Training resources</a></li> </ul>
<b>Government Accountability Office</b>	<ul style="list-style-type: none"> <li>• <a href="#">U.S. Government Accountability Office, Cybersecurity</a></li> </ul>
<b>National Institute of Standards and Technology</b>	<ul style="list-style-type: none"> <li>• <a href="#">Framework for Improving Critical Infrastructure Cybersecurity</a></li> <li>• <a href="#">Internal/Interagency Reports (NISTIRs)</a></li> <li>• <a href="#">National Initiative for Cybersecurity Education (NICE)</a></li> <li>• <a href="#">NICE Cybersecurity Workforce Framework</a></li> </ul>
<b>Various Industry and Associations</b>	<ul style="list-style-type: none"> <li>• <a href="#">ATIS Industry Best Practices</a></li> <li>• <a href="#">Association of Public-Safety Officials, International (APCO), specifically SPCO Cybersecurity Guide for Public Safety Community Professionals and APCO Introductory Guide to Cybersecurity for PSAPs ISACA COBIT 5 Framework</a></li> <li>• <a href="#">ITU Security Standards Roadmap</a></li> <li>• <a href="#">Center for Internet Studies (CIS) Critical Security Controls (CSC), available through the Multi-State Information Sharing and Analysis Center</a></li> <li>• <a href="#">National Association of State Chief Information Officers (NASCIO) Cybersecurity Awareness, including NASCIO Cyber Disruption Planning Guide for States</a></li> <li>• <a href="#">National Conference of State Legislation Cybersecurity Training for State Employees</a></li> <li>• <a href="#">Open Web Application Security Project (OWASP) Top Ten Project</a></li> <li>• <a href="#">OWASP Internet of Things Project</a></li> </ul>

## **Continuity and Resilience**

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

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

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

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

**Table B-4. Continuity and Resilience Resources**

Resource	Description
<b>FEMA National Continuity Programs</b>	<a href="#">National Continuity Programs</a> highlight the national policy and guidance for continuity of operations initiatives. They provide guidance and assistance to support continuity preparedness for federal departments and agencies; state, local, tribal, and territorial government jurisdictions; and private sector organizations.
<b>CISA Regional Resiliency Assessment Program</b>	The <a href="#">Regional Resiliency Assessment Program</a> is a cooperative assessment of specific critical infrastructure within a designated geographic area. DHS works with selected areas each year to conduct a regional analysis of surrounding infrastructure and address a range of resilience issues that could have significant regional or national consequences if disrupted.
<b>CISA Ten Keys to Obtaining a Resilient Local Access Network</b>	This <a href="#">document</a> introduces resiliency concepts and provides ten keys to obtaining and maintaining resiliency in a local access network, such as knowing the exact network infrastructure in the local loop, interfacing with commercial service providers, and properly maintaining alternative path solutions. CISA developed these ten fundamental steps, supported by descriptive text and visually-appealing graphics, as recommendations to help organizations maintain critical communications in emergency situations.
<b>CISA Public Safety Communications Resiliency Self-Assessment Guidebook</b>	This <a href="#">document</a> provides a self-assessment methodology for public safety entities to identify and address potential points of failure in their communication networks by evaluating the local access networks of their primary and alternate operating facilities. The methodology describes the process of gathering data on network infrastructure, creating logical and physical network maps, and choosing resiliency solutions based on the network maps. DHS also developed a <a href="#">Resiliency Fact Sheet</a> to understand communications continuity planning and offer resources to assist entities.
<b>CISA Priority Services Programs</b>	<a href="#">Priority Services Programs</a> , including the Telecommunications Service Priority, Government Emergency Telecommunications Service, and Wireless Priority Service, support national leadership, federal, state, local, tribal, and territorial governments; first responders; and other authorized national security and emergency preparedness users. They are intended to be used in an emergency or crisis situation when data, landline, or wireless networks are congested and the probability of completing a normal transmission or call is reduced.
<b>CISA Electromagnetic Pulse (EMP) Guidance</b>	The <a href="#">EMP Protection and Resilience Guidelines for Critical Infrastructure and Equipment</a> provides guidelines to assist federal, state, and local officials and critical infrastructure owners and operators to protect mission essential equipment against EMP threats. There are four EMP Protection Levels defined. These levels were initially developed at the request of the federal Continuity Communications Managers Group, but are applicable to any organization that desires to protect its electronics and critical infrastructures.

<b>Land Mobile Radio</b>	<p>Grant recipients should purchase digital LMR systems and equipment compliant with the Project 25 (P25) suite of standards (Telecommunications Industry Association), and include all applicable P25 standards and expectations for interoperability in any SOW or acquisition documents</p> <p>Recipients should purchase P25 compliant systems and equipment that has been assessed as compliant in accordance with the P25 Compliance Assessment Program</p> <p>If encryption is required, agencies shall ensure compliance with the P25 Block Encryption Protocol standard and implement Advanced Encryption Standard 256-bit encryption</p> <p>Recipients should ensure all P25 eligible equipment, features, and capabilities selected are P25 compliant, to include new equipment and upgrades</p> <p>When purchasing bridging or gateway devices that have a VoIP capability to provide connectivity between LMR systems, those devices should, at a minimum, implement either the Bridging System Interface specification or the ISSI</p> <p>Recipients should consult the federal granting agency before submitting requests for ISSI and broadband-related project investments to determine whether costs are allowed, as well as applicable technical standards</p>
----------------------------------	---

LMR systems are terrestrially-based, wireless, narrowband communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works companies, and the military in non-tactical environments, to support voice and low-speed data communications. These systems are designed to meet public safety's unique mission and critical voice requirements and support time-sensitive, lifesaving tasks, including sub-second voice call-setup, group calling capabilities, high-quality audio, and priority access to the end-user. Because LMR systems implemented by the public safety community support responders' safety and lifesaving operations, they are designed and implemented to achieve high levels of reliability, redundancy, coverage, and capacity, and can operate in harsh natural and man-made environments. LMR technology has progressed over time from conventional, analog voice service to complex systems incorporating digital and trunking features. These enhancements have improved the interoperability, spectral efficiency, security, reliability, and functionality of voice and low speed data communications.

For the foreseeable future, the public safety community is expected to follow a multi-path approach to develop, establish, and maintain critical communications capabilities. To improve interoperability across investments, grant recipients are strongly encouraged to ensure digital voice systems and equipment purchased with federal grant funds are compliant with the Project 25 (P25) suite of standards, unless otherwise noted in a program's grant guidance.<sup>65</sup> Recipients should ensure all P25 eligible equipment, features, and capabilities selected are P25 compliant, to include new equipment and upgrades. When federal grant funds are used to purchase P25 LMR equipment and systems that contain non-standard features or capabilities, while a comparable P25 feature or capability is available, recipients must ensure the standards-based feature or capability is included.

---

<sup>65</sup> Applicants should read grant guidance carefully to ensure compliance with standards, allowable cost, documentation, reporting, and audit requirements. If interested in using federal funds to purchase equipment that does not align with P25 standards or does not appear on the approved equipment list, the applicant should consult with the federal grant-making agency to determine if non-P25 compliant equipment is allowable. In some cases, written justification must be provided to the grantor. Many agencies will not approve non-standards-based equipment unless there are compelling reasons for using other solutions. Authorizing language for most emergency communications grants strongly encourages investment in standards-based equipment. Funding requests by agencies to replace or add radio equipment to an existing non-P25 system (e.g., procuring new portable radios for an existing analog system) will be considered if there is a clear rationale why such equipment should be purchased and written justification of how the equipment will advance interoperability and support eventual migration to interoperable systems. Written justification should also explain how that purchase will serve the needs of the applicant better than equipment or systems that meet or exceed such standards. Absent compelling reasons for using other solutions, agencies should invest in standards-based equipment.

Grant recipients should purchase P25 compliant systems and equipment that has been assessed in accordance with the P25 Compliance Assessment Program (P25 CAP). P25 standards provide many technical specifications designed to ensure equipment is interoperable regardless of manufacturer. Recipients should obtain documented evidence of P25 compliance from the manufacturer that the equipment has been tested and passed all the applicable, published, normative P25 compliance assessment test procedures for performance, conformance, and interoperability as defined in the latest P25 Compliance Assessment Bulletins for testing requirements. If documentation for applicable equipment is not available through the P25 CAP or there is an absence of applicable testing in the P25 CAP, recipients should obtain documented evidence from the manufacturer stating that the applicable tests were conducted in accordance with the published test procedures in the P25 suite of standards and successfully passed.

### ***Encryption***

Recipients using federal funds to purchase encryption options for new or existing communications equipment shall ensure encrypted capabilities are compliant with the published P25 Block Encryption Protocol Standard. Recipients investing in encryption must implement the Advanced Encryption Standard (AES) 256-bit Encryption Algorithm as specified in the P25 Block Encryption Protocol. The P25 suite of standards references the use of AES as the primary encryption algorithm but continues to allow Data Encryption Standard-Output Feedback (DES-OFB) for backwards compatibility and interoperability with existing systems. The current version of the P25 Block Encryption Protocol, ANSI/TIA-102.AAAD should be identified in all procurement actions when encryption is required.

Recipients seeking to use federal grant funds to purchase non-standard encryption features (e.g., 40-bit encryption, DES-OFB) or capabilities for new or existing equipment must ensure AES 256-bit is also included to ensure their devices have the capability to interoperate in an encrypted mode. Agencies currently using DES-OFB may continue to invest in this encryption method but should plan to migrate to AES as soon as possible. The continued use of DES-OFB or other non-standard encryption algorithms is strongly discouraged. The Federal Government recognizes AES as a more robust encryption algorithm and strongly recommends entities migrate to AES as it will enhance interoperability with federal entities, as well as state and local agencies implementing encryption in the future.

### ***Interconnecting Systems***

When purchasing bridging or gateway devices that have a VoIP capability to provide connectivity between LMR systems, those devices should, at a minimum, implement either the Bridging System Interface (BSI) specification or the P25 Inter Radio Frequency Sub-System Interface (ISSI)/Console Sub-System Interface (CSSI) as a part of their VoIP capability. Note, there are potential interoperability issues when implementing ISSI/CSSI, as testing parameters are still under development and vendors/manufacturers may interpret accredited technical standards differently or may test interfaces inconsistently.

While baseline standards for ISSI connections exist, they are not complete. Due to the current lack of completed accredited technical standards and differing manufacturer's features and functionality implementation practices, public safety agencies should consider planning and technical complexities associated with the implementation of ISSI technologies to connect RF-subsystems (RFSS) from the same or dissimilar LMR vendors/manufacturers. As such, grant applicants should:

- Ensure that operability and interoperability between existing RFSS/systems remain intact and operational during implementation;
- Identify explicit requirements of features, functionalities, and capabilities that the ISSI connections will support to a same or dissimilar manufacturer's RFSS/systems, including interoperability requirements, in any SOW or acquisition documents;

- State the vendor/manufacturer's ability and acceptance to provide these explicit features, functionalities, and capability requirements for ISSI implementation in the appropriate purchasing agreement or contract;
- Develop a set of compliance testing of currently available accredited technical standards criteria with ISSI partners and the selected vendor/manufacturer. Testing should demonstrate standards compliance, as well as successful operability and interoperability functions on each side of the ISSI connection, consistency with procurement and acquisition requirements, and compliance with agreed upon standards;
- Accomplish the set of applicable testing with ISSI partners and the selected vendor/manufacturer that demonstrates successful and effective operability and interoperability of the agreed to features, functions, and capabilities on each side of the ISSI connection, consistent with the stated requirements of the SOW or acquisition documents;
- Submit evidence to the federal granting agency upon successful testing and certification of compliance to applicable accredited technical standards, as well as operability and interoperability with ISSI partners.

Applicants may also be interested in using grant funds to enable interoperability between existing LMR and long-term evolution (LTE) broadband networks. Note, technical standards for interconnecting LMR to LTE systems remain under development. Agencies should beware of proprietary solutions offered by vendors/manufacturers that may provide LMR to LTE connections. However, these proprietary solutions, while achieving LMR to LTE interoperability, are not interoperable amongst themselves thus creating an LTE interoperability issue. Additionally, the indiscriminate, non-planned use of some LTE to LMR Over the Top (OTT) Push to Talk (PTT) solutions has proven to be detrimental to hosting LMR regional/state systems and created significant operability issues and site loading issues for the systems infrastructure. Investing in proprietary solutions is a misuse of federal funds, as additional solutions are needed to restore interoperability among neighboring jurisdictions.

Grant applicants should consult the federal granting agency *before* submitting requests for ISSI/CSSI and broadband-related project investments to determine whether costs are allowed, as well as applicable technical standards.

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

**Table B-5. Land Mobile Radio Standards and Resources**

Organizations	Standards and Resources
<b>P25 Compliance Assessment Program</b>	<a href="#">P25 CAP</a> is a partnership of DHS, industry, and the emergency response community. It is a formal, independent process for ensuring communications equipment declared by the supplier is P25 compliant and tested against standards with published results. It publishes Compliance Assessment Bulletins on policy, testing, and reporting requirements, and an approved equipment list that may be eligible for grants.
<b>Telecommunications Industry Association</b>	<a href="#">TIA</a> is a recognized American National Standards Institution responsible for publishing the P25 suite of standards, approved by the P25 Steering Committee. To date, it has published over 90 documents detailing the specifications, messages, procedures, and tests applicable to the 11 interfaces, multiple feature sets, and functions offered by P25.
<b>SAFECOM Website</b>	<a href="#">SAFECOM Technology Resources</a> provide guidance and recommendations on communications technologies currently used in the public safety environment, including P25 and LMR encryption, ISSI Fact Sheet, P25 ISSI and CSSI Primer, Best Practices for Planning and Implementation of P25 ISSI and CSSI, Volume I.

## **Public Safety Broadband**

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

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

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

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

Applicants should coordinate with the FirstNet Authority in advance of any strategic acquisition of LTE equipment to ensure understanding of all requirements and restrictions impacting broadband investments and that purchases support future service choices. Applicants should also monitor federal actions affecting broadband investments and continue planning and outreach activities (e.g., community education, documenting user needs), as well as work with applicable governing bodies in preparing for and leveraging broadband and other advanced technologies, including:

- Leveraging broadband devices including smartphones, feature phones, tablets, wearables, laptops, ruggedized smartphones, ruggedized tablets, USB modems/dongles, in-vehicle routers, and Internet of Things devices;
- Employing customer-owned and managed broadband deployable equipment, enabling public safety to own and dispatch coverage expansion or capacity enhancement equipment within their jurisdiction;
- Using broadband device accessories that enable efficient and safe public safety operations such as headsets, belt clips, ear pieces, remote Bluetooth sensors, and ruggedized cases;
- Installing standards-based equipment to provide interworking between LTE and existing LMR systems within their jurisdiction when needed;
- Installing FirstNet SIM/UICC cards to allow public safety users to update existing devices, “Bring Your Own Device,” and new devices to operate on public safety prioritized services; and
- Securing one-time purchase and subscription-based applications for public safety use, which could include, among several other options, enterprise mobility management, mobile Virtual Private Network, identity services, or cloud service tools.

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

Upon taking into account these cautions, applicants may be able to use federal grant funds for costs related to the implementation of alternative broadband technologies and the deployment of fiber optic backhaul networks in rural and unserved areas. Applicants should work closely with the federal granting agency and commercial suppliers and providers to ensure that grant-funded systems and equipment will be compatible

and interoperable with current and future solutions. Applicants are encouraged to implement innovative solutions that improve communications capabilities and are consistent with the deployment of the NPSBN.

**Table B-6. Broadband Technology Standards and Resources**

<b>Organizations</b>	<b>Standards and Resources</b>
<b>FirstNet Authority</b>	The Middle Class Tax Relief and Job Creation Act of 2012 created the FirstNet Authority as an independent authority within the National Telecommunications and Information Administration to provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety: <a href="https://www.firstnet.gov">https://www.firstnet.gov</a> .
<b>3GPP</b>	<a href="#">3GPP</a> is the SDO responsible for development and maintenance of LTE specifications, though various standards from TIA, ATIS, the Groupe Speciale Mobile Association (GSMA), and the Open Mobil Alliance (OMA) also contribute to LTE functionality and interoperability.
<b>IEEE</b>	The 802.11a, 802.11b/g/n, and 802.11ac wireless standards are collectively known as Wi-Fi technologies and developed and maintained by IEEE. The <a href="#">Official IEEE 802.11 Working Group Project Timelines</a> provides status of each networking standard under development, and a link to each effort. IEEE also maintains the WiMAX family of 802.16 standards.
<b>Open Geospatial Consortium (OGC)</b>	<a href="#">OGC</a> is an international non-profit organization committed to making quality open standards for the global geospatial community. These standards are made through a consensus process and are freely available for anyone to use to improve sharing of the world's geospatial data.

## Alerts, Warnings, and Notifications

	<p>Grant recipients using funds to cover costs associated with AWN systems should:</p> <ul style="list-style-type: none"><li>• Establish strong governance and engage in collaboration with existing AWN stakeholders</li><li>• Ensure well-documented and field-tested plans, policies, and procedures, are executed, evaluated for potential gaps, and adapted to evolving AWN capabilities</li><li>• Invest in secure and resilient AWN solutions, and incorporate safeguards to ensure the accuracy of messaging</li><li>• Consider diversity and inclusion influence accessibility to AWN issuances, as well as how people receive, interpret, and respond to messages</li><li>• Invest in solutions that enable comprehensive, targeted, specific, and transparent messaging, while minimizing issuance and dissemination delays</li><li>• Select software or equipment that also supports regional operable and interoperable solutions</li></ul> <p>If accessing IPAWS, grant recipients should select equipment and applications that adhere to both Common Alerting Protocol and IPAWS CAP Profile standards, as well as meet the IPAWS minimum critical capabilities</p>
--	---

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

FEMA built IPAWS to ensure that under all conditions the President of the United States can alert and warn the public. Federal, state, local, tribal, and territorial authorities can also use IPAWS to send alerts and warnings within their jurisdictions. IPAWS improves alert and warning capabilities by allowing Alerting Authorities to deliver alerts simultaneously through multiple communications pathways, reaching as many people as possible to save lives and protect property. These communication pathways include:

- [Emergency Alert System \(EAS\)](#) used by authorities to send detailed warnings via broadcast, cable, satellite, and wireline radio and television channels;
- [Wireless Emergency Alerts \(WEA\)](#) sent to mobile devices as a 90- to 360-character message with a unique tone and vibration, even when cellular networks are overloaded and can no longer support person-to-person calls, texts, or emails;
- [National Weather Service Dissemination Systems](#), including the National Oceanic and Atmospheric Administration (NOAA) Weather Radio;
- [Unique Alert Systems](#), such as siren systems and wall beacons, that have permission to retrieve alerts directly from IPAWS and deliver the alerts to their customer base; and
- [Future Systems](#), including computer gaming systems, digital signs, Internet search engines, social sharing websites, wireless device applications, smart home technologies, and others that are or could use IPAWS.

In order to access IPAWS, grant recipients should select equipment and applications that adhere to both the Common Alerting Protocol (CAP) and IPAWS CAP Profile standards, as well as meet the IPAWS minimum critical capabilities. Alert and warning software and equipment is developed, produced, and distributed by various vendors. While the Federal Government does not endorse any specific vendor, piece of software, or equipment, grant recipients should confirm vendors meet CAP and IPAWS CAP Profile standards, provide training and support services, include basic security measures (e.g., firewalls, anti-virus tools, anti-spyware tools), implement strong access controls requiring authentication of users, and connect to the IPAWS Training and Demonstration environment. A key consideration is access to the

service through jammed or damaged communications channels during a real emergency. Recipients should also consider factors affecting continuity of operations, such as support of remote employees, mobile alerting capabilities, and contingent operations in disruptive circumstances.

To maintain AWN issuance proficiencies, agencies sending alerts should conduct trainings, exercises, and tests of systems on a regular basis. Lessons observed from these activities and incidents should be evaluated, documented, and incorporated into future operations. Alert originators should also work to minimize issuance delays, from the point of a hazard's detection to dissemination, by creating message templates, expediting information sharing, identifying and establishing triggers, and avoiding ad-hoc decision making.

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

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

**Table B-7. AWN Standards and Resources**

Organizations	Standards and Resources
<b>Common Alerting Protocol (CAP)</b>	The <a href="#">CAP</a> standard is an open, non-proprietary digital format for exchanging emergency alerts that was developed by Organization for the Advancement of Structured Information Standards (OASIS). CAP allows a consistent alert message to be disseminated simultaneously over many different dissemination mechanisms. The CAP format is compatible with emerging technologies, such as web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' NOAA Weather Radio and the EAS, while offering enhanced capabilities including images, maps, and video.
<b>OASIS</b>	FEMA worked with <a href="#">OASIS</a> to develop a standardized international technical data profile that defines a specific way of using the standard for the purposes of IPAWS. The CAP standard and supplemental IPAWS CAP Profile ensure compatibility with existing warning systems. Latest CAP: <a href="https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#tc-tools">https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#tc-tools</a> .
<b>FEMA Integrated Public Alert and Warning System (IPAWS)</b>	The IPAWS Program Management Office (PMO) does not endorse any specific vendor, piece of software, or equipment. Test results for any alert and warning software or equipment tested at the IPAWS Lab can be made available to assist agencies in making procurement decisions by contacting the IPAWS PMO at <a href="mailto:ipaws@fema.dhs.gov">ipaws@fema.dhs.gov</a> .
<b>Public Safety Communications Ten Keys to Improving Emergency Alerts, Warnings &amp; Notifications</b>	This <a href="#">document</a> provides organizations a series of governance, coordination, planning, cybersecurity, and resiliency best practices to help ensure the successful implementation of their emergency AWN systems and programs. Government and non-government emergency managers, alert originators, system administrators, system operators, and managers can leverage this foundational guidance to deliver timely and actionable messaging during the critical moments of an incident when coordinated communications—down to the second—can save lives.

## 911 Systems

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

- Read the [NG911 Standards Identification and Review](#) and select a Standard Development Organization's standards
- Consult with the National 911 Program Office regarding any updated standards
- Select IP-enabled 911 open standards equipment and software

The National 911 Program, administrated by the Department of Transportation National Highway Traffic Safety Administration (NHTSA), provides federal leadership and coordination in supporting and promoting optimal 911 services. This federal home for 911 plays a critical role by coordinating federal efforts that support 911 services across the Nation. The Implementation Coordination Office, jointly operated by the NHTSA and NTIA, administers a grant program, specifically for the benefit of 911 emergency communication centers (ECCs)/public safety answering points (PSAPs).

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

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

**Table B-8. NG911 Standards and Resources**

Organizations	Standards and Resources
<b>National 911 Program Office</b>	The <a href="#">National 911 Program</a> also provides the 911 community with a collection of documents, website links and other resources generated by both the program and other industry experts. These vetted resources address topics including emerging emergency communications technologies, wireless deployment, E911 location accuracy, cybersecurity, FirstNet, NG911, governance and 911 legislation, and are located in the <a href="#">Document and Tools</a> section of the National 911 Program's website.
<b>NG911 Maturity State Self-Assessment Tool</b>	This <a href="#">Self-Assessment Tool</a> helps ECC/PSAP administrators and oversight personnel evaluate a system's NG911 maturity state and understand the next steps necessary to continue deployment. It contains a detailed, easy-to-use NG911 readiness checklist that establishes common terminology and identifies key milestones to help 911 call centers understand the multi-year NG911 implementation process. The tool is a downloadable Microsoft Excel file, which ensures that collected results are only shared with the agency completing the assessment. The tool translates the answers from ECC/PSAP personnel into one of six maturity states: Legacy, Foundational, Translational, Intermediate, Jurisdictional End State, or National End State. Adopting and sharing the tool's terminology allows for improved communication—with vendors, industry colleagues, elected officials, and others—at the user's discretion.
<b>911 Grant Program</b>	The Middle Class Tax Relief and Job Creation Act of 2012 authorized \$115 million for a targeted 911 Grant Program administered by the Departments of Transportation and Commerce. Visit <a href="https://www.911.gov/project_911grantprogram.html">https://www.911.gov/project_911grantprogram.html</a> for information. Other federal programs fund 911; for a list of federal grant and loan programs that may allow 911 activities, visit: <a href="https://www.911.gov/federal_grants_opportunities.html">https://www.911.gov/federal_grants_opportunities.html</a> .
<b>National Emergency Number Association (NENA) Security for NG911 Standard</b>	Standards of note for NG911 networks include NENA-STA-010: Detailed Functional and Interface Specification for the NENA i3 Solution; NENA 75-001: NENA Security for NG911 Standard (NG-SEC); NENA 75-502: NG-SEC Audit Checklist; NENA 04-503: Network/System Access Security Information Document, and NENA-INF-015.1-2016: NG911 Security Information Document. <a href="http://www.nena.org/">http://www.nena.org/</a> .
<b>NG911 Standards Identification and Review</b>	Collection of resources from all major standards bodies that address cybersecurity when planning for NG911 deployments: <a href="https://www.911.gov/project_standardsforenhancedandnextgeneration911.html">https://www.911.gov/project_standardsforenhancedandnextgeneration911.html</a> .

## Data Exchange and Information Sharing Environments

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

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

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

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

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

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

- [Global Reference Architecture](#) provides guidance for agencies to develop and establish a service-oriented architecture for public safety information sharing. The GRA incorporates and reuses appropriate subsets of the NIEM, as well as other models such as the Global Federated Identity and Privilege Management (GFIPM) sponsored by the Departments of Justice and Homeland Security. The GRA provides practitioners with overarching guidance that demonstrates how federal initiatives, including NIEM and GFIPM, work together and how to accelerate the planning process. Agencies can use this GRA tool to develop a well-conceived, formal approach to designing information sharing solutions and systems. A key benefit of a reference architecture is it helps promote consistent thinking and approaches among the people who use it, even if they have not shared information with each other.
- [OASIS EDXL](#) suite of data messaging standards facilitates information sharing among public safety agencies. Grant-funded systems, developmental activities, or services related to emergency response information sharing should comply with the following OASIS and HL-7 standards: "OASIS EDXL-TEP" and Bi-directional Transformation of OASIS EDXL-TEP (Tracking of Emergency Patients) v1.1 and HL7 v2.7.1 Specification Version and OASIS EDXL suite of data messaging standards. Compliance should include the following OASIS EDXL standards:
  - Common Alerting Protocol, version 1.2 or latest version
  - Distribution Element (DE), version 1.0 or latest version

- Hospital Availability Exchange (HAVE), version 1.0 or latest version
- Resource Messaging (RM) standards, version 1.0 or latest version

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

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

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

A few of the widely used exchange models are provided as part of this appendix; however, an evaluation of who the organization most often communicates with, and what types of information are commonly exchanged, is recommended in selecting an ideal data exchange and information sharing solution. In the future, this evaluation will be assisted by the SAFECOM/NCSWIC ISF document, anticipated for publication in 2020. Additional ISF information will be incorporated in the *FY 2021 SAFECOM Guidance on Emergency Communications Grants*.

**Table B-9. Data Exchange Standards and Resources**

Organizations	Standards and Resources
<b>NIEM</b>	Applicants are encouraged to reference the <a href="#">NIEM website</a> to develop a greater understanding of data exchange functions and processes.
<b>GRA</b>	Many Department of Justice grant solicitations require its grant recipients to comply with the GRA, specifically the Global Standards Package, which describes a full information sharing technology standards implementation suite that addresses data standardization, messaging architecture, security, and privacy requirements. For additional information, including technical assistance and training opportunities, visit the Office of Justice Programs website at: <a href="https://it.ojp.gov/initiatives/gra">https://it.ojp.gov/initiatives/gra</a> .
<b>OASIS</b>	OASIS Emergency Management Technical Committee (EM-TC) creates incident- and emergency-related standards for data interoperability: Common Alerting Protocol; Emergency Data Exchange Language Distribution Element (EDXL-DE); Emergency Data Exchange Language Resource Messaging (EDXL-RM); Emergency Data Exchange Language – Tracking of Emergency Clients (EDXL-TEC). <a href="https://www.oasis-open.org/">https://www.oasis-open.org/</a> .
<b>Information Sharing Assessment Tool</b>	The <a href="#">Information Sharing Assessment Tool</a> , developed by DHS with the guidance of local, state, and federal public safety practitioners, is a tool for public safety officials and first responders to identify their own information sharing capabilities and gaps. It aims to empower communities to develop an action plan to address their most pressing information-sharing gaps; publicize their progress and achievements; and facilitate inter-agency and cross-discipline information sharing.

## Appendix C – Emergency Communications Resources

---

This appendix provides links to references in the *SAFECOM Guidance* and additional resources to help grant applicants develop emergency communications projects and complete federal grant applications. Visit the SAFECOM website (<https://www.dhs.gov/safecom>) for additional resources.

### 911 / Next Generation 911 (NG911)

- National 911 Program Website: <https://www.911.gov/>
  - 911 Grant Program: [https://www.911.gov/project\\_911grantprogram.html](https://www.911.gov/project_911grantprogram.html)
  - *NG911 Standards Identification and Review*: [https://www.911.gov/documents\\_tools.html](https://www.911.gov/documents_tools.html)
  - *NG911 Self-Assessment Tool*: [https://www.911.gov/project\\_ng911tool.html](https://www.911.gov/project_ng911tool.html)
  - Webinars: <https://www.911.gov/webinars.html>
  - Federal Funding Programs for 911: [https://www.911.gov/federal\\_grants\\_opportunities.html](https://www.911.gov/federal_grants_opportunities.html)
- National Association of State 911 Administrators: <http://www.nasna911.org> and <http://www.nasna911.org/state-911-contacts>
- National Emergency Number Association: <https://www.nena.org>
- NG911 NOW Coalition: <http://www.ng911now.org/>

### Cybersecurity

- See [Appendix B in the SAFECOM Guidance](#)
- *NIST Framework for Improving Critical Infrastructure Cybersecurity*: <https://www.nist.gov/cyberframework>
- CISA Cyber Resilience Review: <https://www.us-cert.gov/ccubedvp/cybersecurity-framework>

### Department of Justice (DOJ) Law Enforcement

- *Law Enforcement Tech Guide for Communications Interoperability*: <http://ric-zai-inc.com/ric.php?page=detail&id=COPS-W0714>
- *Law Enforcement Tech Guide Resources for Technology Project Management*: <http://ric-zai-inc.com/ric.php?page=detail&id=COPS-CD040>

### Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Website: <https://www.cisa.gov/>
- Contact Information: [ECD@cisa.dhs.gov](mailto:ECD@cisa.dhs.gov)
- Identity, Credential, and Access Management Resources and *Trustmark Framework*: <https://www.dhs.gov/safecom/icam-resources>
- *National Emergency Communications Plan*: <https://www.cisa.gov/necp>
- National Interoperability Field Operations Guide: <https://www.dhs.gov/safecom/field-operations-guides>
- Priority Services Programs:
  - Government Emergency Telecommunications Service: <https://www.cisa.gov/government-emergency-telecommunications-service-gets>
  - Wireless Priority Service: <https://www.cisa.gov/wireless-priority-service-wps>
  - Telecommunications Service Priority: <https://www.cisa.gov/telecommunications-service-priority-tsp>
- Technical Assistance and Training Catalogs: <https://www.cisa.gov/cisa/interoperable-communications-technical-assistance-program>, <https://www.dhs.gov/safecom/public-safety-software-tools>, and <https://www.dhs.gov/training-technical-assistance>

### Federal Communications Commission (FCC)

- FCC Public Safety and Homeland Security Bureau: <https://www.fcc.gov/public-safety-and-homeland-security>
- Contact Information: [pshsinfo@fcc.gov](mailto:pshsinfo@fcc.gov)
- FCC Fee Filing Guide for the Wireless Telecommunications Bureau: <https://www.fcc.gov/licensing-databases/fees/application-processing-fees>

- FCC Narrowbanding Website: <https://www.fcc.gov/narrowbanding-overview>
- Communications Security Reliability and Interoperability Council: <https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-v>
- Task Force on Optimal Public Safety Answering Point Architecture: <https://www.fcc.gov/encyclopedia/task-force-optimal-public-safety-answering-point-architecture-tfopa>
- FCC 700 MHz Public Safety Broadband Spectrum Guidance: [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-14-172A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-172A1.pdf)
- FCC 800 MHz Transition: <http://transition.fcc.gov/pshs/public-safety-spectrum/800-MHz/>
  - 800 MHz Transition Administrator Website: <http://www.800ta.org/>
  - 800 MHz Transition Administrator Contact: [comments@800TA.org](mailto:comments@800TA.org)
- Middle Class Tax Relief and Job Creation Act of 2012 states T-Band relocation must take place no later than two years after the auction is complete. The Act requires that the auction begin by 2021; however, the deadline for relocation depends on how long the auction takes. For more information, see: <http://www.gpo.gov/fdsys/pkg/BILLS-112hr3630enr/pdf/BILLS-112hr3630enr.pdf>
- Narrowbanding and T-Band Guidance
  - [SAFECOM Guidance, Section 3.3](#)
  - FCC Public Safety T-Band Fact Sheet: <https://www.fcc.gov/file/14462/download>
  - Guidance for licensees for FCC's narrowband operation requirement: <https://www.fcc.gov/narrowbanding-overview>
  - Information on Frequency Coordinators:
  - Contact Information: [narrowbanding@fcc.gov](mailto:narrowbanding@fcc.gov)

### Federal Emergency Management Agency (FEMA)

- FEMA Grants Website: <https://www.fema.gov/grants>
  - Authorized Equipment List: <http://www.fema.gov/authorized-equipment-list>
  - Information Bulletins: <https://www.fema.gov/grants/grant-programs-directorate-information-bulletins>
  - *Preparedness Grants Manual*: <https://www.fema.gov/media-library/assets/documents/178291>
- *Comprehensive Preparedness Guide 201*: <https://www.fema.gov/media-library/assets/documents/165308>
- Environmental Planning and Historical Preservation (EHP): [SAFECOM Guidance, Section 4.5 - Additional Requirements and Recommendations for Equipment Purchases](#)
  - For questions on EHP for DHS/FEMA grants, contact: [GPDEHPInfo@fema.gov](mailto:GPDEHPInfo@fema.gov)
  - For information on federal EHP requirements, see the Council on Environmental Quality Regulations, 40 CFR Part 1500-1508: [https://energy.gov/sites/prod/files/NEPA-40CFR1500\\_1508.pdf](https://energy.gov/sites/prod/files/NEPA-40CFR1500_1508.pdf)
- Integrated Public Alert and Warning System (IPAWS) Program Office: <https://www.fema.gov/integrated-public-alert-warning-system>
  - Alerting Authorities and State, Local, Tribal, and Territorial Users: <https://www.fema.gov/integrated-public-alert-warning-system-authorities>
  - Common Alerting Protocol: <https://www.fema.gov/common-alerting-protocol>
  - Information Materials: <https://www.fema.gov/informational-materials>
  - IPAWS Components: <https://www.fema.gov/ipaws-components>
  - IPAWS Modernization Act of 2015: <https://www.congress.gov/bill/114th-congress/senate-bill/1180>
- Presidential Policy Directive-8: <https://www.dhs.gov/presidential-policy-directive-8-national-preparedness> and <https://www.fema.gov/learn-about-presidential-policy-directive-8>
- National Incident Management System (NIMS): <https://www.fema.gov/national-incident-management-system>
  - NIMS National Standard Curriculum Training Development Guidance: <https://www.fema.gov/nims-training>
  - Communications-Specific Tabletop Exercise Methodology: <https://www.dhs.gov/safecom/resources-library>
- National Preparedness Goal: <https://www.fema.gov/national-preparedness-goal>
- National Preparedness System: <https://www.fema.gov/national-preparedness-system>
- Stakeholder Preparedness Review: <https://www.fema.gov/stakeholder-preparedness-review>
- State Administrative Agency Contact List: <https://www.fema.gov/media-library/assets/documents/28689>

- State Homeland Security Director Office Information: <https://www.dhs.gov/state-homeland-security-contacts>
- Threat and Hazard Identification and Risk Assessment: <https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment>
- Training: <https://www.fema.gov/training> and <https://www.firstrespondertraining.gov>
  - Homeland Security Exercise and Evaluation Program: <https://www.fema.gov/media-library/assets/documents/32326>
  - Incident Command System Resource Center: <http://training.fema.gov/EMIWeb/IS/ICSResource/index.htm>

### **Federal Grants Information and Listings**

- Office of Management and Budget Circulars, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards: <https://www.govinfo.gov/app/details/CFR-2014-title2-vol1/CFR-2014-title2-vol1-part200>
- Grants.gov Website: <https://www.grants.gov>
- FEMA Grants: <https://www.fema.gov/grants>
- SAFECOM compiled list of annual federal financial assistance funding emergency communications: <https://www.dhs.gov/safecom/funding>

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

- FirstNet Authority Website: <https://www.firstnet.gov/>
- FirstNet Authority Contact Information: [outreach@firstnet.gov](mailto:outreach@firstnet.gov)
- NTIA Public Safety Website: <http://www.ntia.doc.gov/category/public-safety>
- Middle Class Tax Relief and Job Creation Act: <http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf>

### **National Public Safety Telecommunications Council (NPSTC): <http://www.npstc.org/>**

- Overview of T-Band issues: <http://www.npstc.org/TBand.jsp>

### **SAFECOM / National Council of Statewide Interoperability Coordinators (NCSWIC)**

- *Emergency Communications System Lifecycle Planning Guide*: <https://www.dhs.gov/safecom/funding>
- *Governance Guide for State, Local, Tribal, and Territorial Emergency Communications Officials*: <https://www.dhs.gov/safecom/governance>
- *Interoperability Planning for Wireless Broadband*: <https://www.dhs.gov/safecom/resources-library>
- *Land Mobile Radio (LMR) Trio – LMR 101, LMR for Decision Makers, and LMR for Project Managers*: <https://www.dhs.gov/safecom/funding>
- *NG911 Self-Assessment Tool*: [https://www.911.gov/project\\_ng911tool.html](https://www.911.gov/project_ng911tool.html)
- *Public Safety Communications Evolution Brochure*: <https://www.dhs.gov/safecom/resources-library>
- *Public Safety Communications: Ten Keys to Improving Emergency Alerts, Warnings & Notifications*: <https://www.dhs.gov/publication/alerts-and-warnings>
- *Public Safety Communications Resiliency: Ten Keys to Obtaining a Resilient Local Access Network*: <https://www.dhs.gov/publication/communications-resiliency>
- *Public Safety Communications Network Resiliency Self-Assessment Guidebook*: <https://www.dhs.gov/publication/communications-resiliency>
- *Regional Interoperability Communications Plan Template*: <https://www.dhs.gov/safecom/resources-library>
- SAFECOM Member List: <https://www.dhs.gov/safecom/membership>
- Statewide Interoperability Coordinator (SWIC): See [SAFECOM Guidance, Sections 3.2](#) and [4.2](#)
- Statewide Communication Interoperability Plan (SCIP): See [SAFECOM Guidance, Sections 2.2](#) and [4.2](#)
  - CISA SCIP Website: <https://www.cisa.gov/statewide-communication-interoperability-plans>
  - To find your SCIP, please contact your SWIC or SCIP Point of Contact. Contact information for SWICs can be found on the NCSWIC membership page: <https://www.dhs.gov/safecom/ncswic-membership>

**Standards**

- SAFECOM Guidance on Technology and Equipment Standards: [SAFECOM Guidance, Section 4.5](#) and [Appendix B](#)
- Association of Public-Safety Communications Officials standards: <https://www.apcointl.org/standards.html>
- Data Exchange and Information Sharing Environment: See [Appendix B in the SAFECOM Guidance](#)
  - National Information Exchange Model: <https://www.niem.gov/Pages/default.aspx>
  - OASIS, Standards for Data-Related Investments: <http://www.oasis-open.org>
  - Information Sharing Assessment Tool: <https://www.dhs.gov/science-and-technology/isat>
- Long-term evolution (LTE) for Public Safety Broadband: See [Appendix B in the SAFECOM Guidance](#)
  - 3GPP RAN5 Mobile Terminal Conformance Testing: <http://www.3gpp.org/specifications-groups/ran-plenary/ran5-mobile-terminal-conformance-testing>
- NIST List of Certified Devices: <https://www.nist.gov/ctl/pscr/process-document-nist-list-certified-devices>
- Project 25 (P25) Standards for Land Mobile Radio: <http://www.tiaonline.org/all-standards/committees/tr-8>
  - P25 Standards for Government Entities: <http://www.tiaonline.org/all-standards/p25-downloads-application>
  - P25 Technology Interest Group: <http://www.project25.org/>
  - P25 Compliance Assessment Program: <https://www.dhs.gov/science-and-technology/p25-cap>
  - P25 Compliance Assessment Program list of approved radio equipment: <https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment>

## Appendix D – Compliance Requirements for DHS Grants

This appendix provides guidance for Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) preparedness grants. Recipients using DHS/FEMA funds for emergency communications activities must comply with the *SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)* in accordance with DHS Standard Terms and Conditions. Table D-1 provides a list of requirements for DHS/FEMA grants. For additional information, see relevant sections within the *SAFECOM Guidance*. DHS/FEMA recipients should also refer to the specific Notice of Funding Opportunity for all programmatic requirements that apply (<https://www.fema.gov/grants>).

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

Topics	Requirements
<b>National and Statewide Plan Alignment</b> Sections 2.2, 2.5, 3.1	<ul style="list-style-type: none"> <li>Describe in applications how proposed projects will support national goals and objectives in the <a href="#">National Emergency Communications Plan (NECP)</a>.</li> <li>Describe in applications how proposed projects will align with your state or territory's <a href="#">Statewide Communication Interoperability Plan (SCIP)</a> goals and objectives. To find your SCIP, contact your Statewide Interoperability Coordinator (SWIC) or SCIP Point of Contact. Contact information for SWICs can be found on the NCSWIC membership page: <a href="https://www.dhs.gov/safecom/ncswic-membership">https://www.dhs.gov/safecom/ncswic-membership</a>.</li> <li>Explain how proposed projects address or support communications resiliency.</li> </ul>
<b>Project Coordination</b> Sections 2.1, 2.2, 2.4, 3.2, 3.3	<ul style="list-style-type: none"> <li>List all participants involved in project planning to demonstrate engagement with the <a href="#">whole community</a> in accordance with <a href="#">Presidential Policy Directive-8</a> and the NECP.</li> <li>Develop regional, multi-jurisdictional, multi-disciplinary, and cross-border projects to promote greater interoperability across agencies, pool grant resources, facilitate asset-sharing, and eliminate duplicate purchases.</li> <li>Designate a full-time SWIC who has the authority and resources to actively improve interoperability with emergency management and response agencies across all levels of government, to include establishing statewide plans, policies, and procedures, and coordinating decisions on communications investments funded through federal grants.</li> <li>Coordinate proposals with statewide emergency communications governance bodies and leaders (e.g., State Interoperability Executive Committee, SWIC, 911 Administrator).</li> </ul>
<b>National Incident Management System (NIMS)</b> Sections 3.4, 4.3, 4.4	<ul style="list-style-type: none"> <li>NIMS Implementation Objectives clarify the specific NIMS implementation criteria to be eligible for FEMA preparedness grants (see: <a href="https://www.fema.gov/implementation-guidance-and-reporting">https://www.fema.gov/implementation-guidance-and-reporting</a>). Some grants may have additional NIMS training or personnel credentialing criteria (see the applicable Notice of Funding Opportunity for details).</li> <li>States, territories, and tribal grant recipients report NIMS implementation annually in the Stakeholder Preparedness Review (SPR). States/territories and tribal grant recipients must submit their annual SPR through the Unified Reporting Tool (URT) and email a copy of the URT submission to their respective DHS/FEMA Regional Federal Preparedness Coordinator and copy <a href="mailto:fema-spr@fema.dhs.gov">fema-spr@fema.dhs.gov</a>. SPR submissions are due no later than December 31st each year.</li> </ul>
<b>Spectrum Licensing</b> Section 3.3	<ul style="list-style-type: none"> <li>If project requires new spectrum license, consult the appropriate statewide coordinator (e.g., SWIC), the Federal Communications Commission, and/or the FirstNet Authority to ensure the recipient will have authority to operate in the desired spectrum. Spectrum consultation should begin prior to application submission or during early phases of an approved project. A spectrum license must be in place before associated equipment can be purchased.</li> </ul>

Topics	Requirements
<b>Planning and Organization</b> Sections 2.2, 3.4, 4.2	<ul style="list-style-type: none"> <li>Update and submit the SPR and Threat and Hazard Identification and Risk Assessment (THIRA). The <a href="#">Comprehensive Preparedness Guide 201</a> provides a three-step process for conducting a THIRA/SPR. Follow THIRA/SPR submission instructions in program guidance.</li> <li>Complete and submit the Nationwide Cybersecurity Review to benchmark and measure progress towards improving cybersecurity posture.</li> </ul>
<b>Training</b> Sections 2.3, 4.3	<ul style="list-style-type: none"> <li>Describe in applications how training projects support the <a href="#">NIMS Training Program</a>, are consistent with NECP priorities, and address gaps identified through your state or territory's SCIP, After-Action Reports, and other assessments.</li> </ul>
<b>Exercises</b> Section 2.3, 4.4	<ul style="list-style-type: none"> <li>Include participants from multiple jurisdictions, disciplines, and levels of government and private sector entities, as appropriate. For additional FEMA exercise guidance, see <a href="https://www.fema.gov/exercise">https://www.fema.gov/exercise</a>.</li> <li>Manage and execute exercises in accordance with the <a href="#">Homeland Security Exercise and Evaluation Program</a>.</li> </ul>
<b>Land Mobile Radio (LMR) Equipment</b> Sections 2.5, 4.5, 5, Appendix B	<ul style="list-style-type: none"> <li>LMR systems are designed to meet public safety's unique mission critical requirements and support time-sensitive, lifesaving tasks, including rapid voice call-setup, group calling capabilities, high-quality audio, and guaranteed priority access to the end-user. For the foreseeable future, the public safety community is expected to follow a multi-path approach to network infrastructure use and development of advanced technologies. Recipients should sustain current LMR capabilities during deployment of advanced technologies in accordance with the NECP.</li> <li>Select Project 25 (P25) standards-based equipment for LMR mission critical voice communications. See the <a href="#">DHS Authorized Equipment List</a> to determine allowable equipment types for DHS/FEMA programs, and the <a href="#">P25 Compliance Assessment Program Approved Equipment List</a>. If proposal includes any non-P25 LMR equipment, recipients must apply for prior approval.</li> </ul>
<b>Next Generation 911 (NG911) Systems</b> Sections 2.5, 4.5, 5, Appendix B	<ul style="list-style-type: none"> <li>NG911 is an Internet Protocol (IP)-based system that allows digital information (e.g., voice, photos, videos, text messages) to flow seamlessly from the public through the 911 network and on to emergency responders. If proposal includes NG911 systems, review the <a href="#">NG911 Standards Identification and Review</a> and select IP-enabled 911 open standards equipment and software. For additional information, consult the National 911 Program Office at <a href="https://www.911.gov/">https://www.911.gov/</a>.</li> </ul>
<b>Public Safety Broadband</b> Sections 2.5, 4.5, 5, Appendix B	<ul style="list-style-type: none"> <li>Consult with applicable governing bodies and leaders for the latest guidance from the FirstNet Authority, planning for public safety broadband network activities, and identifying the authority to operate on public safety spectrum. For additional information, refer to <a href="https://www.firstnet.gov/">https://www.firstnet.gov/</a>.</li> </ul>
<b>Alerts, Warnings, and Notifications</b> Sections 2.5, 4.5, 5, Appendix B	<ul style="list-style-type: none"> <li>The <a href="#">Integrated Public Alert and Warning System</a> (IPAWS) is a modernization and integration of the Nation's alert and warning infrastructure. Federal, state, local, tribal, and territorial alerting authorities can use IPAWS and integrate local systems that use Common Alerting Protocol standards with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System, Wireless Emergency Alerts, the National Oceanic and Atmospheric Administration Weather Radio, and other public alerting systems from a single interface. If proposal includes alerts and warnings, review IPAWS informational materials and Common Alerting Protocol standard at <a href="https://www.fema.gov/informational-materials">https://www.fema.gov/informational-materials</a>.</li> </ul>

## CALIFORNIA GOVERNOR'S OFFICE OF EMERGENCY SERVICES

FY 2020 State Homeland Security Grant Program  
Grant Number #2020-0095 CalOES ID# 107-00000

Subgrantee name: \_\_\_\_\_ Project: \_\_\_\_\_

### **REQUEST FOR SOLE SOURCE PROCUREMENT AUTHORIZATION**

1. Project name: \_\_\_\_\_ Project Budget: \$\_\_\_\_\_
2. Describe the project and/or activity that will be provided by the proposed sole source vendor/contractor.
3. Describe your organization's standard procedures when sole source contracting is considered, including the conditions under which a sole source contract is allowed, and any other applicable criteria (i.e. approval requirements, monetary thresholds, etc.).
4. Indicate which of the following circumstances resulted in your organization's need to enter into a sole source contract.
  - a. Item/service is only available from one source (Describe the process used to make that determination. Please provide details.)
  - b. A public urgency or emergency will not permit a delay resulting from competitive solicitation. According to the US Department of Homeland Security/FEMA, "Time constraints will not be considered a factor if the subgrantee has not sought competitive bids in a timely manner." (Describe the urgency or emergency. Please provide details)
  - c. After solicitation of a number of sources, competition was determined inadequate. (Describe the solicitation process that determined competition was inadequate. Please provide details, and attach any relevant supporting material, Request for Proposal, etc.)
5. Did your organization confirm that the contractor/vendor is not debarred or suspended?
6. Will your organization be able to complete all activities associated with the sole source contract by the end of the grant performance period?
7. Has your organization determined the costs are reasonable?
8. Please attach a copy of the cost benefit analysis prepared for this procurement.

Submitted by \_\_\_\_\_  
(Name) \_\_\_\_\_  
(Signature) \_\_\_\_\_ Date: \_\_\_\_\_

# **TULARE COUNTY DEPARTMENTS BUDGET AND PAYMENT INFORMATION**

**You will need to adjust your Department's budget when you receive your Homeland Security Grant Award Letter IF object line 9610 OR 9800 (whichever pertains to your agency or unit) is not open.**

All Journal Vouchers (JV's) between County Departments beginning with the same Fund Line of 001 must use the following object lines:

**FUND-AGNY-UNIT-OBJ**

**001-xxx-xxxx-9610 (This is the JV entry for you)**

xxx=Your AGENCY number.

xxxx=Your UNIT number

001-142-6082-9510 (This is the Offset JV entry for OES)

**IF** your Department is within Tulare County HHSA, then you will need to use the following object lines:

**FUND-AGNY-UNIT-OBJ**

**001-142-xxxx-9800 (This is the JV entry for you)**

xxxx=Your UNIT number

001-142-6082-9700 (This is the Offset JV entry for OES)

Please see the attached Board Agenda Item regarding FY 2020 State Homeland Security Grant Acceptance and its accompanying AUD308 for more information.