THE HOMELAND SECURITY GRANT PROGRAM

November 2020

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

What's on the Menu?

1. Key Changes
2. FY 2020 HSGP Application revisions
3. Program Guidance
4. 1033 and 1122 Program
5. Procurement

Key Changes: FY2020 National Priorities

Investment in National Priorities:

- For FY 2020, States, Territories, and Urban Areas are required to designate one Investment Justification (IJ) for each of the four National Priorities

- **Each** of the four priority-aligned IJs must equal or exceed **5%** of the applicable State, Territory, or Urban Area's target allocation

Key Changes: FY2020 National Priorities

1. Enhancing cybersecurity **(5%)**
2. Enhancing the protection of soft targets/crowded places **(5%)**
3. Enhancing information and intelligence sharing and cooperation with federal agencies **(5%)**
4. Addressing emerging threats **(5%)**

Equates to **20%** of HSGP award

FY19 IJs VS. FY 2020 IJs

Strengthen Capabilities of the State Threat Assessment System	**IJ # 1**	Enhance Intelligence and Information Sharing and Cooperation With Federal Agencies Including DHS **(National Priority)**
Protect Critical Infrastructure and Key Resources (includes Food and Agriculture)	**IJ # 2**	Enhance Protection of Soft Targets / Crowded Place (including election security) **(National Priority)**
Enhance Cybersecurity	**IJ # 3**	Enhance Cybersecurity **(National Priority)**
Strengthen Emergency Communications Capabilities Through Planning, Governance, Technology, and Equipment	**IJ # 4**	Address Emergent Threats **(National Priority)**
Enhance Medical and Public Health Preparedness	**IJ # 5**	Enhance Medical and Public Health Preparedness
Preventing Violent Extremism Through Multi-Jurisdictional/Inter-Jurisdictional Collaboration and Coordination	**IJ # 6**	Strengthen Emergency Communications Capabilities Through Planning, Governance, Technology, and Equipment
Enhance Community Resilience, Including Partnerships With Volunteers and Community Based Organizations and Programs	**IJ # 7**	Enhance Community Resilience, Including Partnerships With Volunteers and Community Based Organizations and Programs
Strengthen Information Sharing and Collaboration	**IJ # 8**	Strengthen Information Sharing and Collaboration (non-Fusion Center)
Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Planning, Response & Recovery Capabilities	**IJ #9**	Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Planning, Response & Recovery Capabilities
Homeland Security Exercise, Evaluation, and Training Programs	**IJ #10**	Protect Critical Infrastructure and Key Resources (includes Food and Agriculture)

FY 2020 IJs

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

Key Changes: IJs

IJ #1: Enhance Intelligence and Information Sharing and Cooperation With Federal Agencies Including DHS (National Priority)	
Core Capabilities	• Intelligence and information sharing
Example Project Type	• Fusion center operations • Information sharing with all DHS components, fusion centers, and other entities designated by DHS • Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition and analysis • Joint training and planning with DHS officials and other entities designated by DHS

Key Changes: IJs

IJ #2: Protect Soft Targets and Crowded Places (including elections security) (National Priority)	
Core Capabilities	• Operational coordination • Public information and warning • Intelligence and information sharing • Interdiction and disruption • Screening, search, and detection • Access control and identity verification • Physical protective measures • Risk management for protection programs and activities
Example Project Type	• Operational overtime • Physical security enhancements

Key Changes: IJs

IJ #3: Enhance Cybersecurity (including election security) (National Priority)	
Core Capabilities	• Cybersecurity • Intelligence and information sharing

Example Project Type	• Cybersecurity risk assessments
	• Projects that address vulnerabilities identified in cybersecurity risk assessments
	  • Improving cybersecurity of critical infrastructure to meet minimum levels identified by CISA
	  • Cybersecurity training and planning
	• Information security systems

Key Changes: IJs

IJ #4: Address Emergent Threats (National Priority)	
Core Capabilities	• Interdiction & disruption • Screening, search and detection • Physical protective measures • Intelligence and information sharing • Planning • Public Information and Warning • Operational Coordination
Example Project Type	• Sharing/leveraging intelligence and information • UAS detection technologies • WMD/IED/CBRNE prevention, detection, response and recovery capabilities

Key Changes: IJs

IJ #6: Strengthen Emergency Communications Capabilities Through Planning, Governance, Technology, and Equipment	
Core Capabilities	• Operational Communications • Planning
Example Project Type	• Radios • Communication Towers • Dispatch • Tactical Interoperable Communications Plan (TICP) updates

Key Changes: IJs

IJ #10: Critical Infrastructure Protection and Key Resources (includes Food and Agriculture)	
Core Capabilities	• Screening, search and detection • Access Control and Identity Verification • Physical protective measures • Planning • Long Term Vulnerability Reduction • Critical Transportation
Example Project Type	• Vulnerability and risk assessments at critical infrastructure sites • Cameras, lighting, gates, bollards, fencing • Access control systems • Critical infrastructure database management

FY2020 Investment Justifications		State Homeland Security Strategy Goal	
1	Enhance Information and Intelligence Sharing and Cooperation with Federal Agencies, including DHS	1	Enhance Information Collection, Analysis, and Sharing, in Support of Public Safety Operations across California
2	Enhance the Protection of Soft Targets/Crowded Places	2	Protect Critical Infrastructure and Key Resources from All Threats and Hazards
3	Enhance Cybersecurity	3	Strengthen Security and Preparedness across Cyberspace
4	Address Emergent Threats	6	Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Catastrophic Planning, Response, and Recovery Capabilities
		10	Prevent Violent Extremism through Multi-Jurisdictional/Inter-Jurisdictional Collaboration and Coordination
5	Enhance Medical and Public Health Preparedness	7	Improve Medical and Health Capabilities
6	Strengthen Communications Capabilities Through Planning, Governance, Technology, and Equipment	4	Strengthen Communications Capabilities through Planning, Governance, Technology, and Equipment
7	Enhance Community Resilience, Including Partnerships with Volunteers and Community-Based Organizations and Programs	5	Enhance Community Preparedness
8	Strengthen Information Sharing and Collaboration	1	Enhance Information Collection, Analysis, and Sharing, in Support of Public Safety Operations across California
9	Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Planning, Response, and Recovery Capabilities	6	Enhance Multi-Jurisdictional/Inter-Jurisdictional All-Hazards Incident Catastrophic Planning, Response, and Recovery Capabilities
		8	Enhance Incident Recovery Capabilities
		11	Enhance Homeland Security Exercise, Evaluation, and Training Programs
10	Protect Critical Infrastructure and Key Resources (including Food & Agriculture)	2	Protect Critical Infrastructure and Key Resources from All Threats and Hazards
		9	Strengthen Food and Agriculture Preparedness

Key Changes: FY2020 National Priority Projects

- National Priority Projects must be reviewed for effectiveness before funds can be obligated or expended on them
- FEMA/DHS and the various subject matter experts are responsible for conducting reviews
- **ALL** modifications for national priority projects MUST be approved by FEMA/DHS

Key Changes: FY2020 National Priorities

- What if an Operational Area is unable to meet the required 20% of funding for national priority invested projects?
- **If** the state meets or exceeds its five-percent requirement for a national priority we will be able to provide some waivers for that particular National Priority

Key Changes:
FY2020 Project Evaluations

FEMA will evaluate FY2020 National Priority projects for effectiveness upon the first (Winter 2020) BSIR. As such, descriptions and milestones will need to detail the following information:

FY2020 Application Evaluation	
Investment Strategy (30%):	• Quality and extent description demonstrates support for the objective of preventing, preparing for, protecting against, and responding to acts of terrorism, meet target capabilities, and reduce the overall risk to the high-risk urban area, the State, or the Nation
Budget (10%):	• Budget plan maximizing effectiveness of grant expenditures

Key Changes:

FY2020 Application Evaluation	
Impact / Outcomes (30%):	• Closing capability gaps identified in the SPR and address national priorities. • Identification and estimated improvement of core capability and the associated standardized target(s) • The ways in which the applicant will measure and/or evaluate improvement
Collaboration (30%):	• How the project helps 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, local governments, and regional and nonprofit partners

2020 Application Revisions

- Subrecipients must revise their 2020 Financial Management Forms Workbook (FMFW) utilizing the newly released FMFW to include the required National Priority projects (5 % per National Priority)
- A waiver may be submitted for any deficit in the national priority categories
- Revised FMFW's must match the subrecipient's Winter BSIR submittal and are due prior to the Winter BSIR submittal

National Priority Project Waiver Request

- We do not recommend requesting a waiver for the national priority requirement
- In the event the state as a whole does not meet the 5% allocation requirement for a **specific** national priority, no waivers can be approved for that **specific** national priority
- Waivers will be processed on a case-by-case basis and are subject to the state meeting its obligations set forth under the NOFO
- Please reach out to your assigned Program Representative if a waiver is still desired

Final Application 2020

- Final Applications will be due January 31, 2021
- The California Supplement to the NOFO will be released soon
- FY 2020 Grant Assurances are already available at the Cal OES website

FY 2021 Advanced Application

- Due to large number of changes involved with implementing the National Priorities, advanced applications are not required
- It is recommended that subrecipients prepare for FY 2021 to have similar requirements regarding the National Priorities but there is no official information at this time

Key Changes: Prohibitions on Telecommunications and Video Surveillance services and equipment

Effective August 13, 2020, DHS/FEMA recipients and subrecipients **may not** use any FEMA grant funds under the HSGP program FY 2020 or previous years to:

- Procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology of any system; or
- Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology of any system; or
- Enter into, extend, or renew contracts with entities that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system.

As mandated by the John S. McCain National Defense Authorization Act.

Key Changes: Prohibitions on Telecommunications and Video Surveillance services and equipment

Per FEMA August 3, 2020 Memo: "Covered telecommunications equipment or services": Video surveillance or Telecommunications equipment or services produced, provided or used by:

- Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- An entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the FBI, reasonably believes to be an owned, controlled by, or connected to the People's Republic of China

Key Changes: Governing Body Resolution (GBR)

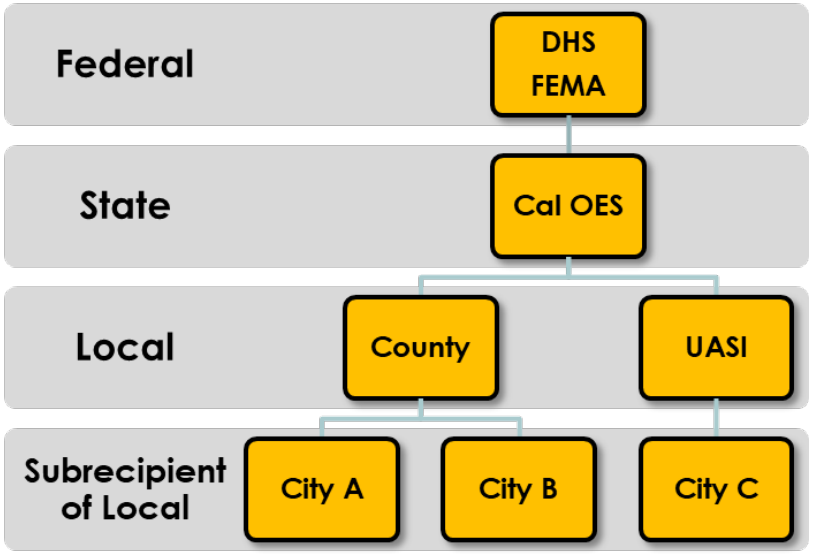
- Can be good for up to three grant years provided that:
  - The resolution identifies the applicable grant program (e.g., EMPG and/or HSGP)
  - The resolution identifies the applicable grant years, (e.g., FY 2020, FY 2021,FY 2022); and
  - Adheres to necessary elements required by local protocols, rules, etc.,if applicable
- Designees can be accepted when authorized by the GBR

Nationwide Cybersecurity Review (NCSR):

- **What:** 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.
  - IB 439 – Supplemental Guidance for Cybersecurity Investments
- **Why:** Evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial governments
- **Result:** DHS bi-yearly anonymous summary report delivered to Congress providing a broad picture of the cybersecurity maturity across communities

Nationwide Cybersecurity Review (NCSR):

- **Who:** Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent for **all** SHSP and UASI subrecipients and subawarded agencies
  - If there is no CIO or CISO, most senior cybersecurity professional should complete NCSR



Nationwide Cybersecurity Review (NCSR):

- **When:** All Subrecipients of SHSP and UASI funding must complete the NCSR between October and December 2020
  - Deadline to Cal OES – **December 16, 2020**
- **How:**
  - Registration required for portal access:
    - https://www.cisecurity.org/ms-isac/services/ncsr/
  - NCSR Portal:
    - https://grc.archer.rsa.com
  - Takes approx. 2-3 hours to complete

NCSR cont.

Required Documentation:

- Cal OES Subrecipients:
  - Submit PDF verifying own NCSR completion
  - AA must certify in writing, on behalf of Subrecipients at next tier, NCSR was completed (list Subrecipients and date completed in a spreadsheet)
- On behalf of your Subrecipients:
  - Ensure you receive certification that NCSR is complete
  - Keep records

Allowable Cost Matrix

Matrix of allowable activities under HSGP (NOFO Pg 31)

Allowable Program Activities	SHSP	UASI	OPSG
Allowable Planning Costs			
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

Personnel Cap:

- SHSP and UASI funds may be used for personnel costs, totaling up to 50% of each fund source
  - Subrecipient may request this requirement be waived by DHS/FEMA, via Cal OES
- Description of Personnel Costs:
  - IB 421, 421a, 421b: Clarification on the Price Act

Personnel Cap:

Personnel Cap Waiver.

- Must be submitted separately for each fund source
- Must be submitted in writing to the Program Representative on official letterhead
- Must address the following information:
  - Documentation explaining why the cap should be waived;
  - Conditions under which the request is being submitted;
  - A budget **and** method of calculation of personnel costs both in percentages of the Grant Award **and** in total dollar amount (include salary, fringe benefits, and any M&A costs)

Personnel Cap:

Example:

HSGP FY2018				
Total SHSP Award	$ 100,000.0			
Total UASI Award	$ 100,000.0			
Total HSGP Award	$ 200,000.0			
Employee	**$SHSP**	**%SHSP**	**$UASI**	**%UASI**
A	$ 10,000	10%	$ -	0%
B	$ 15,000	15%	$ 5,000	5%
C	$ 20,000	20%	$ 5,000	5%
D	$ 25,000	25%	$ 5,000	5%
Total	**$ 70,000**	**70%**	**$ 15,000**	**15%**

UASI Requirements

- States, territories and high-risk Urban Areas complete a Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) for all 32 core capabilities
  - As of FY2019, a THIRA must be submitted every three years
  - SPR continues on an annual basis

UASI Requirements

- UASI Final Applications to Cal OES, must:
  - Include the Urban Area footprint
  - Include the Roster of UAWG Members
  - Ensure projects tie to a State Investment

Fusion Center Requirements

- Fusion Center Projects must align to and reference performance areas of the annual Fusion Center Assessment
- Fusion Center Projects will be reviewed by DHS Office of Intelligence and Analysis
- Fusion Center Analysts must have qualifications that meet or exceed competencies identified in the Common Competencies for State, Local, and Tribal Intelligence Analysts
- Cal OES Director's Letter, dated March 16, 2016

Emergency Communications

- Projects must be compliant with SAFECOM Guidance (updated annually)
- Emergency Communication Projects will be reviewed by:
  - Statewide Interoperability Coordinator (SWIC) at Cal OES; and
  - DHS Office of Emergency Communications
- Emergency Communications Guidance
  - Preparedness Grant Manual 2.0 Appendix A-26

Emergency Communications

- Projects must align with the Statewide Communication Interoperability Plan (SCIP)
- Identify the SCIP Goal # within the Project Description
- Project Description **must** contain the words "Emergency Communications" to easily be identified
- Example:

  Purchase (6) dual-band handheld radios for the city Police Department to enhance interoperability with other public safety agencies ***Emergency Communications (SCIP Goal #3)***

California Statewide Communications Interoperability Plan (Cal-SCIP)

SAFECOM Category	Cal-SCIP Goal
Governance	1. Streamline interoperability planning efforts
	2. Review, update, ensure consistency, and distribute policies and procedures as necessary, to all levels and disciplines (including IT)
Technology	3. Develop a common interoperability platform that leverages existing technology and infrastructure, and provides a migration toward emerging technologies*
	4. Encourage collaboration between Operational Areas and provide opportunities to demonstrate innovative interoperability solutions
	5. Leverage CASM and similar shared resources
Training & Exercises	6. Develop a framework and regularly test interoperability equipment across all disciplines and encourage local adoption
	7. Provide interoperable communications training opportunities using qualified instructors*
	8. Establish a working group to oversee all-hazards communications unit certification
Outreach & Information Sharing	9. Maintain and enhance outreach program to leverage interoperability-related activities, including social media*
	10. Develop a mechanism for succession planning*
	11. Promote CASM and similar shared resources
Life-Cycle Funding	12. Continue to identify a sustainable funding mechanism to support the following priorities*: • Training • SWIC position • CalSIEC efforts • Planning Area support

California Statewide Communications Interoperability Plan (Cal-SCIP)