



Hawaii Office of Homeland Security

FY 2022 Homeland Security Preparedness Grants Meeting

17 December 2021





AGENDA:

- Overview of the Homeland Security Preparedness Grant Programs
 - Homeland Security Grant Program
 - SHSP, UASI, Operation Stone Garden
 - Port Security Grant Program
 - Non-Profit Security Grant Program
- State and Local Cybersecurity Grant Program Overview
- Grant Timelines
- Questions / Discussions



- Issued by the US Department of Homeland Security, Federal Emergency Management Agency Grants Program Directorate
- Annual appropriation from Congress
- Appropriation has specific mandates once the budget is signed 60 days to issue Notice of Funding Opportunity
 - Stipulates timeframe to submit application

OVERVIEW

- The HSGP is a primary funding mechanism for building and sustaining national preparedness capabilities.
- The HSGP supports preparedness activities that address high priority preparedness gaps across all core capabilities that support terrorism preparedness activities, including planning, organization, equipment purchase, training, exercises, and management and administration across all core capabilities and mission areas.
- The basis for funding projects must have a nexus to terrorism
- Period of Performance 36 Months
- No match required
- The HSGP is comprised of three interconnected grant programs (SHSP, UASI and OPSG).

State Homeland Security Program (SHSP)

- This program provides funding to support the implementation of risk-driven, capabilities-based State Homeland Security Strategies to address capability targets.
- 80/20 Split (80% to Counties 20% to State) with 25% supporting law enforcement agencies.

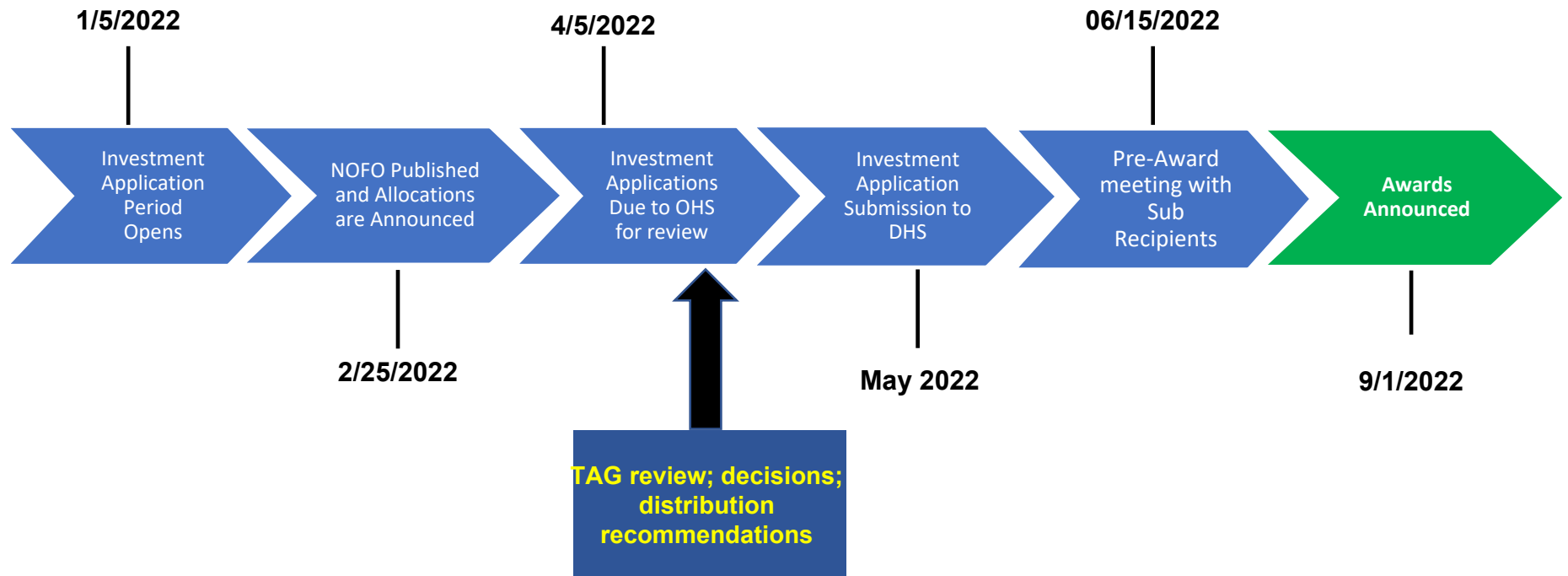
Urban Area Security Initiative (UASI)

- This program provides funding to enhance regional preparedness and capabilities in designated high-threat, high-density areas.
- City and County of Honolulu is the only recipient of the UASI

Operation Stonegarden (OPSG)

- This program provides funding to enhance cooperation and coordination among state, local, tribal, territorial, and federal law enforcement agencies to jointly enhance security along the United States land and water borders

OHS | Projected F22 HSGP Grant Timelines



FY 2021 HSGP GRANT PROGRAMS AWARDED

Program	Grant Amount	Sub Recipients/Management
Homeland Security	\$4,602,500	City and County of Honolulu, Hawaii County, Kauai County, Maui County, DPS, Judiciary, UH, AG, DBEDT-FTZ & DOD
UASI	\$3,800,000	City and County of Honolulu
Port Security*	Federal: \$490,145 State: \$163,382	Department of Transportation
NonProfit**	\$150,000	Kawaiaha'o Church
EMPG***	\$3,562,346	HI-EMA

OHS | Homeland Security Grant Program (HSGP)



FY 2021 HSGP GRANT PROGRAMS PROJECTS

Sub Recipient	Investment	Project Name	Funding Level
DEM-HESD/EMS	(8) Emergency Response Operations	HESD/EMS: Responder Rehab Trailer support in MCI	\$ 240,000.00
DEM-HFD	(9) Infrastructure Systems	Network Upgrade for HFD	\$ 340,000.00
KEMA	(6) Emergency Communications	County Emergency Communication Enhancements	\$ 200,000.00
KEMA	(10) Planning Program and Project Support Training/Exercises	County Cyber Security Enhancements	\$ 370,000.00
HCDA	(6) Emergency Communications	Emergency Alert Messaging	\$ 100,000.00
HCDA-HCPD	(7) Law Enforcements	Law Enforcement Storage Expansion	\$ 500,000.00
HCDA	(10) Planning Program and Project Support Training/Exercises	Citizen Corps Program	\$ 20,000.00
MEMA-DIT	NP 1 - Enhancing Cybersecurity	Cyber Security and Information Systems Resiliency Phase II	\$ 345,187.00
MEMA-MPD	(6) Emergency Communications	Public Information and Warning	\$ 53,516.00
MEMA	(8) Emergency Response Operations	EOC Response Vehicles	\$ 120,000.00
MEMA- Dept of Management	(10) Planning Program and Project Support Training/Exercises	County of Maui COOP Update	\$ 100,000.00
MEMA-MFD	(10) Planning Program and Project Support Training/Exercises	IMAT	\$ 25,000.00
DPS	(6) Emergency Communications	P25 Communication Capabilities Enhancements	\$ 100,000.00
	(7) Law Enforcements	Deployable Mobile Command/Operational Assets	\$ 50,000.00
UH - Manoa Department of Public Safety	NP 2 - Enhancing the Protection of Soft Targets / Crowded Places	UHM-DPS Integrated Security Platform	\$ 124,000.00
AG-HCJDC	(7) Law Enforcements	NCIC Message Switch Hardware Refresh	\$ 124,000.00
Judiciary	NP 2 - Enhancing the Protection of Soft Targets / Crowded Places	Judiciary Gunshot Detection Program	\$ 109,000.00
DBEDT-FTZ	(9) Infrastructure Systems	FTZ No. 9 Access Control	\$ 200,000.00
OHS-Fusion	NP 3 - Enhancing Information and Intelligence Sharing	Hawaii State Fusion Center	\$ 230,125.00
OHS	NP 4 - Combatting Domestic Violent and Extermism	Combating Domestic Violent Extremism - Targeted Violence and Terrorism Prevention	\$ 345,187.00
OHS	NP 5 - Addressing Emergent Threats	Interdependent Critical Infrastructure Common Operating Picture	\$ 230,125.00
OHS-SWIC	(6) Emergency Communications	Statewide Communications Interoperable Planning	\$ 50,000.00
OHS-Planning	(10) Planning Program and Project Support Training/Exercises	Homeland Security Planning	\$ 296,360.00
OHS-Training/Exercises	(10) Planning Program and Project Support Training/Exercises	Training and Exercises	\$ 100,000.00
OHS-M&A	(10) Planning Program and Project Support Training/Exercises	Homeland Security M&A	\$ 230,000.00



NP 1 - Enhancing cybersecurity (7.5%)

NP 2 - Enhancing the protection of soft targets/crowded places (5%)

NP 3 - Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies, including DHS (5%)

NP 4 - Combating domestic violent extremism (5%)

NP 5 - Addressing emergent threats (e.g., transnational criminal organizations, unmanned aircraft systems [UASs], weapons of mass destruction [WMD], etc.) (5%)





NATIONAL PRIORITIES PROJECT EXAMPLES

Priority Areas	Core Capabilities	Lifelines	Example Project Types
Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies, including DHS	<ul style="list-style-type: none"> Intelligence and information sharing Interdiction and disruption Planning Public information and warning Operational coordination Risk management for protection programs and activities 	<ul style="list-style-type: none"> Safety and Security 	<ul style="list-style-type: none"> Fusion center operations (Fusion Center project will be required under this investment, no longer as a stand-alone investment) Information sharing with all DHS components; fusion centers; other operational, investigative, and analytic entities; and other federal law enforcement and intelligence entities Cooperation with DHS officials and other entities designated by DHS in intelligence, threat recognition, assessment, analysis, and mitigation Identification, assessment, and reporting of threats of violence Joint intelligence analysis training and planning with DHS officials and other entities designated by DHS
Combating Domestic Violent Extremism	<ul style="list-style-type: none"> Interdiction and disruption Screening, search and detection Physical protective measures Intelligence and information sharing Planning Public information and warning Operational coordination Risk management for protection programs and activities 	<ul style="list-style-type: none"> Safety and Security 	<ul style="list-style-type: none"> Open source analysis of misinformation campaigns, targeted violence and threats to life, including tips/leads, and online/social media-based threats Sharing and leveraging intelligence and information, including open source analysis Execution and management of threat assessment programs to identify, evaluate, and analyze indicators and behaviors indicative of domestic violent extremists Training and awareness programs (e.g., through social media, suspicious activity reporting [SAR] indicators and behaviors) to help prevent radicalization Training and awareness programs (e.g., through social media, SAR indicators and behaviors) to educate the public on misinformation campaigns and resources to help them identify and report potential instances of domestic violent extremism
Addressing Emergent Threats, such as the activities of Transnational Criminal Organizations, open source threats, and threats from UAS and WMD	<ul style="list-style-type: none"> Interdiction & disruption Screening, search and detection Physical protective measures Intelligence and information sharing Planning Public Information and Warning Operational Coordination 	<ul style="list-style-type: none"> Safety and Security 	<ul style="list-style-type: none"> Sharing and leveraging intelligence and information UAS detection technologies Enhancing WMD and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities <ul style="list-style-type: none"> Chemical/Biological/Radiological/Nuclear/Explosive (CBRNE) detection, prevention, response, and recovery equipment

NP - 3

NP - 4

NP - 5



NATIONAL PRIORITIES PROJECT EXAMPLES

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			
<p>Enhancing Cybersecurity</p> <p>NP - 1</p>	<ul style="list-style-type: none"> • Cybersecurity • Intelligence and information sharing • Planning • Public information and warning • Operational coordination • Screening, search, and detection • Access control and identity verification • Supply chain integrity and security • Risk management for protection programs and activities • Long-term vulnerability reduction • Situational assessment • Infrastructure systems • Operational communications 	<ul style="list-style-type: none"> • Safety and Security 	<ul style="list-style-type: none"> • Cybersecurity risk assessments • Migrating online services to the “.gov” internet domain • Projects that address vulnerabilities identified in cybersecurity risk assessments <ul style="list-style-type: none"> ○ Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency (CISA) ○ Cybersecurity training and planning
<p>Enhancing the Protection of Soft Targets/ Crowded Places</p> <p>NP - 2</p>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Safety and Security 	<ul style="list-style-type: none"> • Operational overtime • Physical security enhancements <ul style="list-style-type: none"> ○ Closed-circuit television (CCTV) security cameras ○ Security screening equipment for people and baggage ○ Lighting ○ Access controls ○ Fencing, gates, barriers, etc.

INVESTMENT JUSTIFICATIONS

NP 1 - Enhancing cybersecurity (7.5%)

NP 2 - Enhancing the protection of soft targets/crowded places (5%)

NP 3 - Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies including DHS (5%)

NP 4 - Combating domestic violent extremism (5%)

NP 5 - Addressing emergent threats (e.g., transnational criminal organizations, unmanned aircraft systems [UASs], weapons of mass destruction [WMD], etc.) (5%)

6 – Emergency Communications

7 – Law Enforcement

8 – Emergency Response Operations

9 – Infrastructure Systems

10 – Planning Program and Project Support Training / Exercises

* Investment for cybersecurity projects will require completion of the Nationwide Cybersecurity Review (NCSR) Assessment. Portal will be closed on **February 28, 2022**

OHS | Homeland Security Grant Program (HSGP)

FY 2021 HSGP DISTRIBUTION - NATIONAL

Total Funding	Distribution		National Priorities 30% Total = \$1,380,750.00					Contribution to Sub recipients (Counties)	Urban Areas Security Initiative (100% Funding to C&C of HNL)
	80%	20%	NP 1 - CYBER SECURITY 7.5% Minimum: \$345,187.50	NP 2 - ENHANCING SOFT PROTECTION 5% Minimum: \$230,125.00	NP 3 - INFORMATION AND INTELLIGENCE SHARING 5% Minimum: \$230,125.00	NP 4 - COMBATING DOMESTIC VIOLENT EXTREMISM 7.5% Minimum: \$345,187.00	NP 5 - EMERGENT THREATS 5% Minimum: \$230,125.00		
\$4,602,500.00	\$3,682,000.00	\$920,500.00	\$345,187.00	\$233,000.00	\$230,125.00	\$345,187.00	\$230,125.00	\$1,268,297.00	\$3,800,000.00
Sub Recipient Distribution									
City and County	\$580,000.00								
County of Maui	\$643,703.00		\$345,187.00						
County of Kauai	\$570,000.00								
Count of Hawaii	\$620,000.00								
Total for Sub Recipients	\$2,413,703.00								
State Distribution									
Attorney General - HCJDC		\$124,000.00							
Foreign Trade Zone		\$200,000.00							
Judiciary, State of Hawaii		\$109,000.00		\$109,000.00					
University of Hawaii - Manoa		\$124,000.00		\$124,000.00					
Department Public Safety		\$150,000.00							
DOD for National Priorities		\$575,312.00				\$345,187.00	\$230,125.00		
DOD Program and Projects		\$296,360.00							
Consortium Training		\$100,000.00							
Hawaii State Fusion Center		\$230,125.00			\$230,125.00				
Statewide Communications Interoperable Planning (SCIP)		\$50,000.00							
Management and Administration (M&A)		\$230,000.00							
Total for State		\$2,188,797.00	\$345,187.00	\$233,000.00	\$230,125.00	\$345,187.00	\$230,125.00		
Contribution Summary									
Contribution Investments	Total	State Funding Portion	Sub Recipient Contribution Portion						
National Priorities (NP 2,4,5)	\$808,312.00	\$100,000.00	\$708,312.00						
Consortium Training	\$100,000.00	\$50,000.00	\$50,000.00						
Fusion Center (NP-3)	\$230,125.00	\$109,956.00	\$120,169.00						
DOD Program and Projects	\$296,360.00	\$118,544.00	\$177,816.00						
Attorney General - HCJDC	\$124,000.00	\$62,000.00	\$62,000.00						
SCIP	\$50,000.00	\$20,000.00	\$30,000.00						
M&A	\$230,000.00	\$110,000.00	\$120,000.00						
Total Contribution Portion for State and Sub Recipients		\$570,500.00	\$1,268,297.00						

FTZ and DPS Projects n/a to sub recipients	\$350,000.00
--	--------------

Total State Portion	\$920,500.00
----------------------------	---------------------



PORT SECURITY GRANT PROGRAM (PSGP) OVERVIEW

Purpose:

The PSGP supports port authorities, facility operator, and state and local agencies for activities associated with implementing the Area Maritime Security Plans, facility security plans and other port-wide risk management efforts.

- PSGP is a Competitive Grant
 - Applicants will be scored
- The PSGP period of performance is three years / 36 months



PSGP FUNDING PRIORITIES (2021)

- Enhancing Cybersecurity
- Second Tier Priorities:
 - 1) Enhancing the protection of soft targets/crowded places;
 - 2) Addressing emerging threats (e.g., transnational criminal organizations, weapons of mass destruction [WMD], unmanned aerial systems [UASs], etc.);
 - 3) Effective planning;
 - 4) Training and awareness campaigns;
 - 5) Equipment and capital projects; and
 - 6) Exercises.



PSGP FUNDING PRIORITIES (2021)

FY 2021 PSGP Funding Priorities

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			
Enhancing Cybersecurity	<ul style="list-style-type: none"> Cybersecurity Intelligence and information sharing Planning Public information and warning Operational coordination Screening, search, and detection Access control and identity verification Supply chain integrity and security Risk management for protection programs and activities Long-term vulnerability reduction Situational assessment Infrastructure systems Operational communications 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Cybersecurity risk assessments Projects that address vulnerabilities identified in cybersecurity risk assessments <ul style="list-style-type: none"> Improving cybersecurity of critical infrastructure to meet minimum levels identified by CISA Cybersecurity training and planning
Enduring Needs			
Enhancing the Protection of Soft Targets and Crowded Places	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Physical security enhancements at cruise and ferry terminals <ul style="list-style-type: none"> Explosive detection canine teams Security cameras (CCTV) Security screening equipment for people and baggage Access controls <ul style="list-style-type: none"> Landside fencing, gates, barriers, etc. Marine (floating) barriers to prevent access to sensitive berthing areas Enhanced security aboard ferries <ul style="list-style-type: none"> Explosive detection canine teams Security cameras (CCTV) Rapid response boats for preventing or responding to security incidents on waterways, especially in and around airports, cruise terminals, ferry terminals, etc.

Priority Areas	Core Capabilities	Lifelines	Example Project Types
Addressing Emerging Threats, such as Transnational Criminal Organizations, WMD and UAS	<ul style="list-style-type: none"> Interdiction and disruption Screening, search and detection Physical protective measures Intelligence and information sharing 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Sharing and leveraging intelligence and information Chemical Biological Radiological Nuclear and Explosive (CBRNE) prevention, detection, response, and recovery equipment UAS detection technologies
Planning	<ul style="list-style-type: none"> Planning Risk management for protection programs and activities Risk and disaster resilience assessment Threats and hazards identification Operational coordination Community resilience 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Development of: <ul style="list-style-type: none"> Port-wide Security Risk Management Plans Continuity of Operations Plans Response Plans Efforts to strengthen governance integration between/among regional partners
Training and Awareness	<ul style="list-style-type: none"> Long-term vulnerability reduction Public information and warning Operational coordination Situational assessment Community resilience 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Active shooter training Shipboard firefighting training Public awareness/preparedness campaigns Maritime domain awareness projects
Equipment and Capital Projects	<ul style="list-style-type: none"> Long-term vulnerability reduction Infrastructure systems Operational communications Interdiction and disruption Screening, search and detection Access control and identity verification Physical protective measures 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Implementing risk management projects that support port resilience and recovery Implementing physical security enhancement projects Transportation Worker Identification Credential (TWIC) projects
Exercises	<ul style="list-style-type: none"> Long-term vulnerability reduction Operational coordination Operational Communications Community resilience 	<ul style="list-style-type: none"> Safety and Security Transportation 	<ul style="list-style-type: none"> Response exercises



ELIGIBILITY REQUIREMENTS

- Eligible applicants:
 - Port Authorities
 - Facility operators: Examples of facility operators include, but are not limited to terminal operators, ferry systems, bar/harbor pilots, and merchant's exchanges.
 - state and local government agencies.
 - Private sector partners
- Investments must support port areas (maritime).
 - Support increase port-wide risk management and protect critical surface transportation infrastructure from acts of terrorism
 - Addresses the NOFO Priorities



ELIGIBILITY REQUIREMENTS

- A single eligible entity may submit only one application within each port area.
 - An application may contain up to five (5) investments
- Cost Match
 - For profit entities must provide a 50 percent match
 - State / Local Government entities must provide a 25 percent match
 - Example: Total project Cost: \$300k
 - \$225,000 - 75% Federal Portion
 - \$75,000.00 - 25% Cash Match (out of own entity's expense)



ELIGIBILITY REQUIREMENTS

- Valid Employer Identification Number (EIN)
 - Dun and Bradstreet Universal Numbering System (DUNS)
 - Active registration in System for Award management (SAM)
- * An eligible entity applying for the grant does not guarantee grant funding



APPLICATION REVIEW PROCESS

- State
 - The local U.S. Coast Guard Captain of the Port (COPT) reviews, prioritized projects and will rate projects after submittal
 - COPT makes recommendation to the DHS /FEMA
- Federal
 - Review
 - Final Scoring
 - Award



APPLICATION SUBMISSION PROCESS

- Eligible entity must complete the Investment Justification Form
- Eligible entity to submit the completed Investment Justification to the State Administrative Agency (SAA) (HIDOD /OHS) for review
- SAA will submit the Investment Justification applications to the USCG COPT and the DHS

Note: The SAA will submit applications on behalf of the eligible entity



REFERENCES:

- PSGP Investment Form Template
<https://dod.hawaii.gov/ohs/grants-2022>
- FY 2021 Port Security Grant Program Notice of Funding Opportunity
https://www.fema.gov/sites/default/files/documents/FEMA_FY2021-PSGP-NOFO_02-18-21.pdf
- System for Award Management:
<https://sam.gov/content/home>



NSGP OVERVIEW

Purpose

The Fiscal Year (FY) 2021 Nonprofit Security Grant Program (NSGP) provides funding support for physical security enhancements (target hardening) to nonprofit organizations that are at high risk of a terrorist attack.

- **NSGP is a Competitive Grant**
 - Applicants will be scored
- **NSGP period of performance is 36 months**
 - Projected Period of Performance Start Date(s): September 1, 2022.
 - Projected Period of Performance End Date(s): August 31, 2025



ELIGIBILITY REQUIREMENTS

- **An organization described under section 501(c)(3) of the Internal Revenue Code of 1986**
 - Organizations such as churches, mosques, and synagogues are considered automatically exempt if they meet the requirements of section 501(c)(3) and do not have to apply for and receive a recognition of exemption from the IRS.
- **Valid Employer Identification Number (EIN)**
- **Dun and Bradstreet Universal Numbering System (DUNS)**
(April 2022 DUNS are not required, registration is all under the SAM)



ELIGIBILITY REQUIREMENTS

- High Risk for Terrorist Attacks
 - Be able to demonstrate, through the application, that the organization is at high risk of a terrorist attack. due to their ideology, beliefs, or mission.
 - Describe any incidents that have occurred at the facility.
 - Describe any threats (e.g., verbal threats, vandalization) made against the organization.
 - Monitor current events with specific attention to incidents impacting organizations that have been targeted due to a similar mission, belief, or ideology.
- Each applicant may apply for up to three different sites
 - Require an Investment Justification for each site
 - Conduct a vulnerability assessment specific to the location / facility that you are applying for (CISA)
 - Ensure that each site does not exceed \$150k / site

Note: Eligibility does not guarantee grant funding



Eligible Project Examples

- **Equipment:**
 - Fencing, Barriers, blast-proof windows, concrete barriers
 - Security Cameras
 - Access Control System
 - Security Screening Equipment
 - Notification and warning systems
 - Radios and Public Address Systems
- **Private Contracted Security Guards**
- **Planning:**
 - Development of plans such as security risk management plans, community of operations plans and response type plans
- **Training:**
 - Active Shooter Training
 - Security training for employees, or members / congregation
- **Exercises:**
 - Response exercises



Ineligible Project Examples

- Overtime and backfill
- Hiring of public safety personnel
- Organizational operating expense
- Reimbursement of pre-award security expenses
- Cameras for license plate readers/ license plate reader software
- Cameras for facial recognition software
- Weapons or weapons-related training
- Knox boxes



Investment Justification (go through IJ form)

- Section 1: Applicant Information
- Section II: Background
- Section III: Risk
- Section IV: Target Hardening
- Section V. Milestones
- Section VI. Project Management
- Section VII. Impact
- Funding History
- Applicant Contact Information



APPLICATION REVIEW PROCESS



- Two-Phased Process:
 - State Administrative Agency (SAA) review
 - Federal Review
- Results used to inform the final funding decision made by the Secretary of Homeland Security



APPLICATION SUBMISSION PROCESS

- Non-Profit organization must conduct a vulnerability Security assessment for each site
- Non-Profit organization must complete the Investment Justification Form
- Non-Profit to submit the completed Investment Justification to the State Administrative Agency (SAA) (HIDOD /OHS) for review
- SAA will submit the Investment Justification applications to the DHS before the application deadline (May 2022)

NOTE: The SAA is the only entity eligible to apply for the NSGP funds on behalf of an eligible Nonprofit organization



REFERENCES:

- NSGP Investment Justification Form Template
<https://dod.hawaii.gov/ohs/grants-2022>
- FY 2021 NSGP Notice of Funding Opportunity
https://www.fema.gov/sites/default/files/documents/fema_fy2021-nsgp-nofo_3-2-2021.pdf
- System for Award Management
<https://sam.gov/content/home>



STATE AND LOCAL CYBERSECURITY GRANT PROGRAM

\$1 billion for the next 4 years starting in FY22:

FY22: \$200 million

FY23: \$400 million

FY24: \$300 million

FY25: 100 million

- 80/20 percent split (80% to local and 20% to State)
- State CIOs and CISOs serve as primary officials to manage and allocate funding **(TBD)**
- 5% can be used for administrative costs, such as salaries and other related expenses
- Plans must be approved by a planning committee and the state CIO/CISO (or equivalent official)
- The Federal share of the cost of an activity carried out using the grant funds made available under the program may not exceed: 90% for FY22, 80% for FY23, 70% for FY 24, 60% for FY25.
 - The State share may not be an in-kind match.



CYBERSECURITY PLAN:

The key item of the grant program and likely guidance for grant application focuses on the submission of a cybersecurity plan, which must be submitted to CISA.

PLANNING COMMITTEES:

States that receive grants shall establish a planning committee to:

1. Assist with the development and implementation of the cybersecurity plan
2. Approve of the cybersecurity plan
3. Assist with the determination of the effective funding priorities for the grant

COMPOSITION OF PLANNING COMMITTEE:

Representatives from the state, counties, cities, towns, institutions of public education and health within the jurisdiction, and Tribes with members from suburban, rural and high-population jurisdictions with no less than half members having professional experience related to cybersecurity or IT.

Any existing planning committee or commission may be used if it meets the requirements and may be expanded or leveraged to meet the requirements.



REPORTING REQUIREMENTS:

- Within 1 year after the date the grant was received, the state must provide a report to DHS CISA, which includes:
- Implementation progress of their approved cybersecurity plan
- If no plan exists, how grant funds were obligated and expended to develop a cybersecurity plan or improve information systems
- Annual reports will be made publicly available and are subject to redactions in order to protect sensitive information.

NEXT STEPS:

- CISA/FEMA Grant Guidance
 - Likely will try to align with the Homeland Security Grant Program (HSGP) timeline
- Continued engagement with associations to solicit feedback and influence grant guidance
- Formal engagement with CISA and SLTT associations



QUESTIONS & DISCUSSION

Office of Homeland Security

Frank Pace, Administrator – frank.j.pace@hawaii.gov

Glen Badua, Grants Manager – glen.m.badua@hawaii.gov

Petronilla Sole, Grant Specialist – petronilla.l.sole@hawaii.gov

Website: www.ohs.hawaii.gov

Phone: (808) 369-3570

