STATE HOMELAND SECURITY GRANT INFORMATION BULLETIN
IB 21.G001
MARCH 10, 2021

PURPOSE

The purpose of this information bulletin is to provide guidance for submitting grant applications that align with the five (5) priority funding investments listed below to be included in Indiana's FFY21 State Homeland Security Grant. IDHS will receive and review the sub-applications ensure that the sub-applications submitted as part of the state application align with the FFY2021 State Homeland Security Grant (SHSP) project scope.

SOLICITATION

To qualify for a FFY2021 SHSP priority funding, applicants must address one of the four priority investments available to sub-recipients, which include cybersecurity, enhancing the protection of soft target/crowded places, combating domestic violent extremism and addressing emerging threats. Applicants also must demonstrate the terrorism nexus to preventing, preparing for, protecting against and responding to acts of terrorism.

Applicants must fill out the application form completely. Projects requested under an investment priority are capped at **$345,187.50 for cybersecurity and domestic violent extremism and $230,125.00 for soft targets/crowded places and emerging threats. The information and intelligence sharing and cooperation priority is restricted to the Indiana Intelligence Fusion Center.** Project requests may be less than the cap, but the state's total investment priority must meet the funding cap. Budgets should be as accurate as possible with no overestimation. It is possible that multiple projects are funded under a singular investment priority, therefore partial funding might be granted. However, the goal is to fund projects in their entirety.

Applications will be **limited to one per organization** with a focus on local law enforcement. The project submitted should only address a single priority. If an EMA is applying on behalf of a police department or other entity and puts the police department as the organization all further paperwork including IntelliGrants accounts will be required to stay in that organization's name.

If an organization is awarded a priority investment, a detailed application and budget will need to be entered into the IntelliGrants system.

INSTRUCTIONS AND DEADLINES

Grant Application Submission Deadline: **April 23, 2021 at 5:00 PM ET**

All proposals/budgets must be submitted through the Indiana Department of Homeland Security Grants Management email at grants@dhs.in.gov by **April 23, 2021 at 5:00 PM EDT.** All fields within the priority funding investment application are required to be complete and must include the correct Authorized Equipment List (AEL) numbers for the purchase of all equipment. The FEMA AEL list can be found online at https://www.fema.gov/authorized-equipment-list.

IDHS expects SHSP applicants to prioritize funding requests to address capability targets and gaps identified through a needs assessment or gap analysis process. Please note, due to limited funding, it is likely that only projects addressing high priority core capability gaps will be considered for award. However, there is no guarantee that all high funding priorities will be funded. Applicants should prioritize the use of grant funds to maintain/sustain current capabilities, to validate capability levels and to increase capability for high priority core capabilities with low capability levels.

Applications submitted after the deadline will not be considered for funding.

APPLICATION SUBMISSION OR APPROVAL DOES NOT GUARANTEE FUNDING

IDHS will review applications that align with funding priorities of agency. IDHS will then submit the priority investment projects to FEMA for review. Final award amounts will be based on U.S. DHS/FEMA's evaluation of the effectiveness of proposed investments and projects.

QUESTIONS

For grant specific questions and technical assistance, please submit a grants support ticket at https://www.in.gov/dhs/grants-management/grants-management/.

ADDITIONAL INFORMATION

Further grant specific information can be found on the IDHS website in the Fiscal Year 2021 Homeland Security Grant Program (HSGP) Notice of Funding Opportunity and FEMA Preparedness Grants Manual, Version 2, February 2021.

PRIORITY FUNDING INVESTMENT JUSTIFICATIONS

1. CYBERSECURITY INVESTMENT JUSTIFICATION

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 sub-recipients of FY 2021 SHSP grant awards will be required to complete the 2021 Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture.

2. SOFT TARGET INVESTMENT JUSTIFICATION

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 the 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.

3. INFORMATION AND INTELLIGENCE SHARING AND COOPERATION INVESTMENT JUSTIFICATION (FUSION CENTER)

Cooperation and information sharing among state, federal and local partners across all areas of the homeland security enterprise, including counterterrorism – including both international and domestic terrorism, cybersecurity, border security, transnational organized crime, immigration enforcement, economic security and other areas is critical to homeland security operations and the prevention of, preparation for, protection against and responding to acts of terrorism, other threats to life and criminal acts of targeted violence. 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 U.S. DHS and other federal agencies. As noted above, this requirement must include at least one dedicated fusion center project. The Indiana Intelligence Fusion Center will fulfill this investment justification.

4. COMBATING DOMESTIC VIOLENT EXTREMISM INVESTMENT JUSTIFICATION

Domestic violent extremists, including ideologically motivated lone offenders and small groups, present the most persistent and lethal terrorist threat to the homeland. These violent extremists capitalize on social and political tensions, which have resulted in an elevated threat environment. They utilize social media platforms and other technologies to spread violent extremist ideologies that encourage violence and influence action within the United States.

The COVID-19 pandemic has further created an environment that may lead to accelerated mobilization to targeted violence and/or radicalization to domestic terrorism, including driving lawful protests to incite violence, intimidate targets and promote their violent extremist ideologies. Given the rise of domestic violent extremism in recent years, at least one investment must be in support of the state's efforts to combat the rise, influence and spread of domestic violent extremism.

5. EMERGING THREATS INVESTMENT JUSTIFICATION

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 production of unmanned aircraft systems, artificial intelligence and biotechnology increase opportunities of threat factors to acquire and use these capabilities against the United States and its interests.

INVESTMENT JUSTIFICATION TABLE

National Priorities	Core Capabilities	Example Project Types
Enhancing cybersecurity	• 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	• Cybersecurity risk assessments • Migrating online services to the ".gov" internet domain • Projects that address vulnerabilities identified in cybersecurity risk assessments • Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency (CISA) • Cybersecurity training and planning
Enhancing the protection of soft targets/crowded places	• 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	• Operational overtime • Physical security enhancements • Closed-circuit television (CCTV) security cameras • Security screening equipment for people and baggage • Lighting • Access controls

	• Risk management for protection programs and activities	• Fencing, gates, barriers, etc.
Enhancing information and intelligence sharing and analysis, and cooperation with federal agencies, including DHS	• Intelligence and information sharing • Interdiction and disruption • Planning • Public information and warning • Operational coordination • Risk management for protection programs and activities	• Fusion center operations (Fusion Center project will be required under this investment, no longer as a stand-alone investment) • Information sharing with all U.S. DHS components; fusion centers; other operational, investigative, and analytic entities; and other federal law enforcement and intelligence entities • Cooperation with U.S. DHS officials and other entities designated by U.S. DHS in intelligence, threat recognition, assessment, analysis, and mitigation • Identification, assessment and reporting of threats of violence • Joint intelligence analysis training and planning with U.S. DHS officials and other entities designated by U.S. DHS
Combating domestic violent extremism	• 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	• 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	• Interdiction and disruption • Screening, search and detection • Physical protective measures • Intelligence and information sharing	• Sharing and leveraging intelligence and information • UAS detection technologies

	• Planning • Public information and warning • Operational coordination	• Enhancing WMD and/or improvised explosive device (IED) prevention, detection, response and recovery capabilities • Chemical/Biological/Radiological/ Nuclear/Explosive (CBRNE) detection, prevention, response and recovery equipment

IDHS CORE CAPABILITY PRIORITIES

IDHS relied on the following reports to prioritize core capabilities for FFY 2021 SHSP grant funding:

- 2020 State Preparedness Report; and
- 2020 Core Capability Assessments.

Based on a review of local capability assessments and the 2020 State Preparedness Report, the list below categorizes projects and its associated core capability based on priority level. **Note**: There are some core capabilities that will not be able to be funded during the FFY 2021 SHSP grant cycle. See **Figure 1.1** for a visual table.

HIGH FUNDING PRIORITIES

- Planning (Prevention/Protection/Mitigation/Response/Recovery)
- Public Information and Warning (Prevention/Protection/Mitigation/Response/Recovery)
- Operational Coordination (Prevention/Protection/Mitigation/Response/Recovery)
- Cybersecurity (Protection)
- Intelligence and Information Sharing (Protection)
- Physical Protective Measures (Protection)
- On-Scene Security, Protection and Law Enforcement (Response)
- Infrastructure Systems (Response/Recovery)
- Screening Search and Detection (Prevention/Protection)
- Access Control and Identity Verification (Protection)
- Public Health, Healthcare and EMS (Response)

MEDIUM FUNDING PRIORITIES

- Logistics and Supply Chain Management (Response)
- Forensics and Attribution (Prevention)
- Interdiction and Disruption (Prevention/Protection)
- Mass Search and Rescue (Response)
- Supply Chain Integrity and Security (Protection)
- Fatality Management Services (Response)
- Environmental Response, Health & Safety (Response)
- Operational Communications (Response)

LOW FUNDING PRIORITIES

- Risk Management for Protection Programs and Activities (Protection)
- Threats and Hazards Identification (Mitigation)
- Situational Assessment (Response)

CORE CAPABILITIES NOT CONSIDERED FOR FUNDING DURING FFY 2021

- Community Resilience (Mitigation)
- Long-Term Vulnerability Reduction (Mitigation)
- Risk and Disaster Resilience Assessment (Mitigation)
- Fire Management and Suppression (Response)
- Critical Transportation (Response)
- Mass Care Services (Response)
- Economic Recovery (Recovery)
- Housing (Recovery)
- Health and Social Services (Recovery)
- Natural and Cultural Resources (Recovery)

To assist in prioritization efforts, IDHS aggregated the FFY 2021 SHSP funding priorities into **Figure 1.1** on the next page.

The core capabilities in green represent the high funding priorities, the core capabilities in yellow represent the medium funding priorities, the core capabilities in red represent the low funding priorities and the core capabilities in grey represent the capabilities not being considered during the FFY 2021 SHSP grant cycle.

PREVENTION	PROTECTION	MITIGATION	RESPONSE	RECOVERY
Planning	Planning	Planning	Planning	Planning
Public Information and Warning	Public Information and Warning	Public Information and Warning	Public Information and Warning	Public Information and Warning
Operational Coordination	Cybersecurity	Operational Coordination	Public Health, Healthcare, and Emergency Management Services	Operational Coordination
Intelligence and Information Sharing	Operational Coordination	Threats and Hazards Identification	Operational Coordination	Infrastructure Systems
Screening, Search, and Detection	Intelligence and Information Sharing	Community Resilience	On-Scene Security, Protection, and Law Enforcement	Economic Recovery
Forensics and Attribution	Physical Protective Measures	Risk and Disaster Resilience Assessment	Infrastructure Systems	Housing
Interdiction and Disruption	Screening, Search, and Detection	Long-Term Vulnerability Reduction	Logistics and Supply Chain Management	Health and Social Services
	Access Control and Identity Verification		Environmental Response, Health, and Safety	Natural and Cultural Resources
	Supply Chain Integrity and Security		Fatality Management	
	Interdiction and Disruption		Operational Communication	
	Risk Management for Protection Programs and Activities		Mass Search and Rescue Operations	
			Situational Assessment	
			Mass Care Services	
			Critical Transportation	
			Fire Management and Suppression	