Mississippi Office of Homeland Security Grant Program (HSGP)
FY22 HSGP Notice of Funding Announcement
February 1, 2022

Purpose:
The purpose of this announcement is to provide guidance for submitting grant applications for the upcoming FY22 Homeland Security grant program. Grant applications must align with the five (5) national priority funding investments listed below.

Solicitation:
To qualify for FY22 priority grant funding, applicants must address one of the five (5) national priority areas available to sub-grantees, which includes cyber-security, enhancing the protection of soft targets/crowded places, enhancing information and intelligence sharing and analysis, combating domestic violent extremism and addressing emergent threats. Applicants must also demonstrate the terrorism framework to prevent, prepare, protect against, and respond to acts of terrorism.

Applicant must fill out the application form, completely. Projects meeting one or more of the national priorities will be considered and reviewed first for funding. Project requests outside the federal priority areas will be considered and reviewed secondary.

Application Release:
The Mississippi Office of Homeland Security (MOHS) will release the FY22 Homeland Security Grant program grant application on **Tuesday, February 15, 2022**. The application, along with the funding guidance document will be available on the MOHS website at: https://www.homelandsecurity.ms.gov/

Grant Writing:
The MOHS will also host two (2) grant writing workshops to answer questions regarding the grant and provide updates on grant funding, priority areas and information about the upcoming FY22 grant year. Dates for the grant writing sessions will be held on **February 28, 2022, and March 8, 2022**. Please R.S.V.P for grant writing by Tuesday, February 22, 2022, to at mohsgrants@dps.ms.gov.

Instructions and Deadlines:
All proposals must be submitted electronically to the MOHS email address at mohsgrants@dps.ms.gov by **April 1, 2022, at 5:00 p.m. CDT**. All fields are required to be completed and must include all required information and signatures for a completed application.

The MOHS requests that all jurisdictions prioritize funding requests to address the capability targets and gaps identified through a needs assessment. Please note, due to limited funding, it is likely that only projects addressing high priority capability gaps and meet the national and state priorities will be funded. Applicant should prioritize the use of grant funds to maintain/sustain current capabilities.

Applications submitted after the deadlines will not be considered for funding but may be considered if funding becomes available. Application submission does not guarantee funding. MOHS will review applications that align with the funding priorities of the agency.

Questions:
For questions related to the grant application, guidelines or need technical assistance, please contact the MOHS email address at mohsgrants@dps.ms.gov.

FEMA Additional Information:
Further grant specific information can be found on the FEMA website at: https://www.fema.gov/media-collection/homeland-security-grant-notices-funding-opportunity

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 FY22 HSGP grant awards will be required to complete the 2022 Nationwide Cybersecurity Review (NCSR), enabling agencies to benchmark and measure progress of improving their cybersecurity posture.

2. Soft Target/Crowded Places Investments 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 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: 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.

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.

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:
The table below shows all national priority investment justifications, along with the core capabilities and example projects for each priority area.

Priority Areas	Core Capabilities	Lifelines	Example Project Types
National Priorities			
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	• Safety and Security	• Cybersecurity risk assessments • Migrating online services to the ".gov" internet domain • Projects that address vulnerabilities identified in cybersecurity risk assessments o Improving cybersecurity of critical infrastructure to meet minimum levels identified by the Cybersecurity and Infrastructure Security Agency (CISA) o 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 • Risk management for protection programs and activities	• Safety and Security	• Operational overtime • Physical security enhancements o Closed-circuit television (CCTV) security cameras o Security screening equipment for people and baggage o Lighting o Access controls o Fencing, gates, barriers, etc.

Priority Areas	Core Capabilities	Lifelines	Example Project Types
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	• Safety and Security	• 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	• 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	• Safety and Security	• 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 & disruption • Screening, search and detection • Physical protective measures • Intelligence and information sharing • Planning • Public Information and Warning • Operational Coordination	• Safety and Security	• Sharing and leveraging intelligence and information • UAS detection technologies • 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