U.S. Department of Homeland Security
Washington, DC 20472

FEMA

Grant Programs Directorate Information Bulletin
No. 429
May 21 2018

MEMORANDUM FOR: All State Administrative Agency Heads
All State Administrative Agency Points of Contact
All Urban Area Security Initiative Points of Contact
All State Homeland Security Advisors
All State Chief Information Security Officers
All State Chief Information Officers
All Urban Area Chief Information Security Officers
All Urban Area Chief Information Officers

FROM: Jeanette Manfra
Assistant Secretary
Office of Cybersecurity and Communications

Thomas DiNanno
Assistant Administrator for Grant Programs
Federal Emergency Management Agency

SUBJECT: **Supplemental Guidance to Inform Cybersecurity Investments Under the FY 2018 Homeland Security Grant Program (HSGP)**

I. Purpose

This Information Bulletin (IB) provides supplemental guidance to inform the development of the required cybersecurity investment justification.

II. Applicability

This IB is applicable to State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) grant recipients.

III. Guidance

A. Beginning in FY 2018, SHSP and UASI grant recipients are required to complete the following actions:

1. Include Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) in Senior Advisory Committees (SAC) and Urban Area Working Groups (UAWG). Inclusion of CIOs and CISOs in the grant decision-making groups ensures cyber threat and risk management expertise is represented in the grant planning and allocation process.

2. At least one (1) investment must be in support of the state's, territory's or urban area's cybersecurity efforts. Recipients must limit the use of grant funds to projects that support the security and functioning of critical infrastructure and core capabilities with a nexus to terrorism preparedness and that may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism.

3. The cyber justification must be a separate and distinct submission that seeks to mitigate an organization-specific gap or vulnerability identified in a Stakeholder Preparedness Report (SPR), Threat Hazard Identification Risk Analysis (THIRA), and/ or more focused cyber assessment, like the Nationwide Cybersecurity Review (NCSR). The NCSR can assist recipients in identifying organization-specific gaps in cyber risk management that support cybersecurity investment justifications (https://www.cisecurity.org/ms-isac/services/ncsr/).

B. Project descriptions in the Investment Justification (IJ) and the Biannual Strategy Implementation Report (BSIR) should provide enough specificity on the need for, and products and/or services provided through, the investment to allow FEMA to understand:

1. the state, territory, or urban area organization being affected by the investment;

2. the threat that the project is intended to mitigate;

3. the capability gap that the project is intended to fill; and,

4. for sustainment projects, the capability level or proficiency the project is intended to sustain.

For examples on the types of cybersecurity resources allowable under the SHSP and UASI program and organized by Planning, Organization, Equipment, Training, Exercise(POETE) element, see Exhibit A: Table 1. For information on the types of cybersecurity activities that produce successful outcomes as organized by the

National Institute of Standards and Technology (NIST) Cybersecurity Framework, POETE element, and activity outputs and outcomes, see Exhibit B: Table 2.

C. Resources

1. DHS strongly recommends participation in its Cyber Hygiene Program:

   a. The no-cost DHS Cyber Hygiene Program provides vulnerability scanning to help secure internet-facing systems from known vulnerabilities, detects insecure configurations, and encourages the adoption of security best practices.

   b. DHS performs regular network and vulnerability scans and delivers a weekly report for your action.

   Once initiated, this service is mostly automated and requires little direct interaction. After DHS receives the required paperwork for Cyber Hygiene, scans start within 72 hours and state, local, tribal, and territorial (SLTT) governments will begin receiving reports within two weeks. SLTT governments can sign up and obtain further details by contacting NCATS_INFO@hq.dhs.gov.

2. DHS has several additional no-cost cybersecurity resources for SLTT governments. From cyber awareness and technical training to vulnerability assessments, there are resources available which do not require the expenditure of grant funds. To help SLTT government leaders get started in building a cybersecurity program, or enhance an existing program, DHS has created resources specifically designed to help leaders recognize and address their cybersecurity risks. Resources include discussion points for government leaders, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to SLTT governments. Many of these resources are described in further detail at https://www.us-cert.gov/ccubedvp/sltt.

3. Additional technical assistance available to SHSP and UASI recipients and subrecipients includes the following:

   a. General Resources

      i. The DHS Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, enhances the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C serves as the hub for each state, territory, and urban area's cybersecurity inquiries and resources. States, territories, and urban areas should review these resources with their CIO and CISO to determine which resources will best serve their community's efforts to build and sustain a robust cybersecurity program.

ii. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (the Framework) provides standards, guidelines, and best practices to promote the protection of critical infrastructure. Grant recipients and subrecipients can use the Framework to align cybersecurity investments to policy, communicate cybersecurity requirements to stakeholders, measure current cybersecurity posture through self-assessment, and analyze trade-offs between expenditure and risk. DHS resources aligned to the Framework Function Areas can be found at https://www.us-cert.gov/ccubedvp/sltt.

iii. Funded by DHS, the Multi-State Information Sharing and Analysis Center (MS-ISAC) improves the overall cybersecurity posture of the Nation's SLTT governments through focused cyber threat prevention, protection, response, and recovery. It is a no-cost, membership-based community that includes 24/7 cybersecurity support, analysis and monitoring, and a central location for reporting threats and suspicious activities. For more on the MS-ISAC, visit https://www.cisecurity.org/ms-isac/ .

b. Training Resources

The Federal Virtual Training Environment (FedVTE) provides more than 800 hours of free online cybersecurity training to U.S. government (including SLTT government) employees, Federal contractors, and veterans. DHS manages the FedVTE program. It is administered through an interagency agreement with the U.S. Office of Personnel Management and supported by the Department of Defense's Defense Information Systems Agency through course development initiatives. Course proficiency ranges from beginner to advanced levels and have topics such as ethical hacking, risk management, and malware analysis. For more information on how to register for courses and obtain a log-in visit https://fedvte.usalearning.gov/.

D. Allowable Cybersecurity Expenditures

Recipients must limit the use of grant funds for projects that support the security and functioning of critical infrastructure and core capabilities as they relate to terrorism preparedness and may simultaneously support enhanced preparedness for other hazards unrelated to acts of terrorism. Examples of allowable cybersecurity expenditures are outlined in Exhibit A: Table 1.

IV. Questions

For questions regarding the SHSP and UASI programs or allowable expenditures, please contact AskCSID@fema.dhs.gov.

For questions related specifically to cybersecurity and developing the cyber-focused investment justification, please contact SLTTCyber@hq.dhs.gov and include "FEMA Grant" in the subject line.

V. Review Date

This IB will be reviewed within two years (2) from date of issuance.

Exhibit A: SHSP and UASI Allowable Cybersecurity Resource Expenditures by POETE Element

Table 1 provides examples of the types of resources that are allowable and encouraged under SHSP and UASI. The resource examples are not meant to be exhaustive and are provided only for consideration.

Table 1. Examples of resources (organized by POETE element) that can be funded through SHSP or UASI

POETE Element	Resource	Examples
Planning	Requirements and standards	Cybersecurity capability assessments
	Current cybersecurity and related response plans	• Cybersecurity Strategy • IT Security Plan • Cybersecurity Incident Response Plan • IT Disaster Recovery Plan
	Risk/configuration assessments	Penetration testing, contracted risk assessors
Organization	Internal personnel	Full time employees such as CISO, ISSO, network administrators, cybersecurity analysts, etc.
	External personnel	Contracted support such as cybersecurity service contractors, etc.
Equipment[1]	Software	Software such as anti-virus, anti-malware, continuous monitoring, encryption, enhanced remote authentication, patch management, distributed denial of service protection, etc.
	Hardware	Hardware such as intrusion detection systems, intrusion prevention systems (firewalls), additional servers, routers/switches, etc.
	Physical protection	Items such as fencing, cameras, locks (including electronic), biometrics readers, etc., to protect access to hardware and systems.
Training	Awareness-level training	Internal or external design, conduct, and evaluation of awareness-level training.
	Cybersecurity professional training	Internal or external design, conduct, and evaluation of professional-level cybersecurity training.
Exercise	Awareness drills	Drill preparation, conduct, and evaluation.
	Response/recovery exercises	Exercise preparation, conduct, and evaluation.

[1] Additional information on specific, pre-approved equipment can be found in the Authorized Equipment List (https://www.fema.gov/authorized-equipment-list).

Exhibit B: Example Cybersecurity Activities by NIST Function, POETE Element, and Outputs

Table 2 provides examples of allowable activities. They are organized by NIST function and POETE element and provide insight into the likely outputs from each activity. This is not an exhaustive list of activities that can be funded through HSGP, but rather strategic guidance to use as a framework in developing a cyber-focused investment justification.

Table 2. Activities, aligned to NIST function and POETE element, and their expected outcomes

NIST Function	Cybersecurity Activity	P	O	E	T	E	Measuring Progress of Outputs • Activity checklist items • Quarterly reports
Identify	Assess cybersecurity risks and threats.	✓					Yearly risk assessments.
	Develop an inventory of networks, devices, data, and systems.	✓					Inventory of networks, deployed hardware, data, and installed software.
	Establish governance structures for steady-state and response operations.	✓	✓				• CIO/CISO integrated in Senior Advisory Committee or Urban Area WG. • Documented information security policy, including legal and regulatory requirements. • Documented roles and responsibilities (e.g., CISO, CIO, CTO).
Protect	Develop mechanisms to manage access to networks, devices, and systems.		✓	✓			Centralized identity and privilege management, such as single sign-on, multi-factor authentication, and disabling/deleting accounts.
	Conduct awareness-level training for end-users.				✓		Awareness training campaigns, such as phishing and insider threat.
	Create and maintain a baseline configuration solution with appropriate security principles.	✓		✓			• Logs centralized, correlated, and consolidated • Logs synchronized with security information and event management (SIEM) software • Incorporated whitelisting
	Implement and test protection processes and procedures.	✓		✓		✓	Protective processes such as network segmentation (e.g., business side from infrastructure networks), privileged access, endpoint protection, public key infrastructure, and key management.
Detect	Set up technology and processes to monitor networks, devices, and system security.	✓		✓			Monitoring processes such as log management, configuration management, whitelisting, patching, and vulnerability management.
	Develop and test technology and processes to detect anomalies and events.			✓		✓	Security Operations Center (performing continuous monitoring functions).
	Set up procedures and organization to communicate anomaly and event detection.	✓	✓	✓			• Intrusion detection systems • Security information and event management solutions

NIST Function	Cybersecurity Activity	P	O	E	T	E	Measuring Progress of Outputs • Activity checklist items • Quarterly reports
Respond	Develop incident response and business continuity plans that incorporate lessons learned.	✓					Current response (including mitigation) and COOP plans.
	Set up procedures and organization to coordinate and communicate mitigation processes to all stakeholders.	✓	✓				Security Operations Center (performing response and mitigation functions).
Recovery	Develop incident recovery and disaster recovery plans that incorporate lessons learned.	✓					• Current recovery plans that incorporate lessons learned • Security Operations Center (performing recovery functions)
	Set up processes by which restoration is coordinated and communicated to all stakeholders.	✓	✓				Data Security