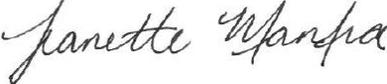


Grant Programs Directorate Information Bulletin
No. 439
April 12, 2019

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 Director
Cybersecurity and Infrastructure Security Agency

Christopher P. Logan 
Acting Assistant Administrator
Grant Programs Directorate
Federal Emergency Management Agency

SUBJECT: Supplemental Guidance to Inform Cybersecurity Investments Under the Fiscal Year 2019 Homeland Security Grant Program

I. Purpose

This Information Bulletin (IB) provides supplemental guidance to inform the development of the required cybersecurity investment justification. This IB supplements IB 429a (July 11, 2018) by introducing the Nationwide Cybersecurity Review (NCSR) as a required assessment, starting with the Fiscal Year (FY) 2019 State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI), the two major funding streams within the FY 2019 Homeland Security Grant Program (HSGP). This IB and the NCSR outline technical and administrative resources for SHSP and UASI recipients and subrecipients to complete and interpret results of the NCSR. This IB is not intended to remove or alter any provisions of IB 429a.

The Federal Emergency Management Agency (FEMA) recognizes the challenges presented by the time constraints of an inconsistent federal funding cycle. Based on stakeholder feedback from across the cybersecurity community, FEMA and the Cybersecurity and Infrastructure Security Agency (CISA) have determined that providing information on the NCSR requirement would benefit and improve the quality of the cybersecurity investment justifications (IJs) submitted by HSGP recipients. The NCSR is 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. The NCSR is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by DHS and the Multi-State Information Sharing and Analysis Center (MS-

ISAC). The anonymous results provide a nationwide snapshot of cybersecurity posture.

II. Applicability

This information bulletin is applicable to SHSP and UASI grant recipients and subrecipients.

III. Guidance

A. SHSP and UASI grant recipients or subrecipients are required to complete the following actions:

1. **Existing requirements:** SHSP and UASI recipients are required to complete the actions described in section III, subsections A and B of IB 429a. SHSP and UASI recipients and subrecipients may refer to section III, subsection D and Exhibits A and B of IB 429a for additional information on allowable cybersecurity expenditures.
2. **NEW requirement:** SHSP and UASI recipients and subrecipients must complete the NCSR by the end of Calendar Year 2019, as outlined in the FY 2019 HSGP Notice of Funding Opportunity (NOFO). The 2019 NCSR will be open from October through December 2019.

IV. Nationwide Cybersecurity Review (NCSR) Requirement Details

A. Background:

The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual users in state, local, tribal, territorial, nonprofit, and private sectors. Using the results of the anonymous NCSR, DHS delivers a biennial summary report to Congress providing a broad picture of the cybersecurity maturity across the state, local, tribal, territorial, nonprofit and public/private communities. The data is also used by DHS to prioritize cybersecurity support provided to state, local, tribal, territorial, nonprofit, and private sectors.

Starting in early 2020, FEMA and DHS will receive an aggregate anonymized summary report providing the current cybersecurity posture of the country. Any specific/identifying information will be removed.

B. Completing the NCSR:

For SHSP and UASI recipients and subrecipients, the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent for each recipient and subrecipient should complete the NCSR. If there is no CIO/CISO, the most senior cybersecurity professional should complete the assessment. Although this is only a requirement for recipients and subrecipients of FY 2019 SHSP and UASI funds, all state, local, tribal, and territorial agencies with preparedness responsibilities are highly

encouraged to participate and complete the 2019 NCSR to evaluate their cybersecurity posture.

The NCSR will be open from October through December 2019 for completion. The NCSR is available at no cost to the user and takes approximately 2-3 hours to complete. Upon completion, users will receive an immediate summary report of results, along with supplemental information from the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The MS-ISAC is available to answer administrative and technical questions and will provide guidance upon release of the FY 2019 NOFOs. Please submit questions about the NCSR to MS-ISAC at ncsr@cisecurity.org.

The MS-ISAC will also host webinars following the release of the NOFO with detailed instructions on completing the NCSR.

For more information about the NCSR, visit: <https://www.cisecurity.org/ms-isac/services/ncsr/>.

C. NCSR Results and FEMA Grants:

Recipients should report completion of the NCSR in their Biannual Strategy Implementation Report (BSIR) as outlined in IB 429a and the FY 2019 HSGP NOFO. FEMA and the DHS will verify completion of the NCSR but will not receive or be able to review specific survey results. Only the user will be able to see its own results. FEMA and DHS will receive an anonymized report providing the current cybersecurity posture of the country, but any specific/identifying information will be removed.

FEMA and DHS require completion of the NCSR to: 1) enhance the quality and increase impactful projects in future investment justifications, and 2) provide policy and decision makers with a snapshot of cybersecurity posture and roadmap to fund improvements over time. The NCSR provides users with actionable feedback on their cybersecurity programs, allowing users to take feedback and develop projects that directly address identified gaps. This method of gap analysis and risk mitigation will allow users to make important and effective cybersecurity improvements.

These results allow policymakers to determine nationwide cybersecurity priorities, and in turn, dedicate necessary resources and funding to support these priorities.

V. Resources

In addition to the resources identified in section III, subsection C of IB 429a, SHSP and UASI recipients and subrecipients may also utilize the following resources.

- A. Funded by DHS, the MS-ISAC improves the overall cybersecurity posture of the nation's state, local, tribal, territorial, nonprofit, and private sector agencies 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. The MS-ISAC is available for both technical and administrative assistance on the NCSR. For more on the MS-ISAC, visit <https://www.cisecurity.org/ms-isac/services/ncsr/> or email ncsr@cisecurity.org.

- B. CISA enhances the security, resilience, and reliability of the Nation’s cyber and communications infrastructure. CISA 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. CISA has cybersecurity resources available at the regional level, providing organization-specific and customized cybersecurity guidance. The Cybersecurity Advisors (CSAs) in the field help prepare and protect private sector entities and state, local, tribal, territorial, nonprofit, and private sector agencies from cybersecurity threats. CSAs promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities. For more information about the CSA Program, email cyberadvsior@hq.dhs.gov.

- C. The NIST CSF provides standards, guidelines, and best practices to promote the protection of critical infrastructure. Grant recipients and subrecipients can use the NIST CSF 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 Cybersecurity Framework Function Areas can be found at <https://www.us-cert.gov/ccubedvp/slitt>.

VI. Questions

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

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.

For questions related specifically to the NCSR or the MS-ISAC, please contact ncsr@cisecurity.org for more information.

VII. Review Date

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