DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2026-0067]

Agency Information Collection Activities: State and Local Cybersecurity Grant Program (SLCGP) Evaluation

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-day notice and request for comments; new collection (request for a new OMB Control Number, 1670–NEW).

SUMMARY: The Stakeholder Engagement Division (SED) Grant Analytics Branch within the Cybersecurity and Infrastructure Security Agency (CISA) submits the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].** Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: You may submit comments, identified by docket number Docket # CISA-2026-0067, by following the instructions below for submitting comment via the Federal eRulemaking Portal at http://www.regulations.gov.

Instructions: All comments received must include the agency name and docket number Docket # CISA-2026-0067. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Jessena Robinson, 202-706-1385,

Jessena.Robinson@cisa.dhs.gov; Ijeoma Mordi, 202-746-2255,

Ijeoma.Mordi@cisa.dhs.gov

SUPPLEMENTARY INFORMATION:

The Foundations for Evidence-Based Policymaking Act of 2018 (Pub. L. 115– 435), or the Evidence Act, promotes the use of evidence to inform decision making and requires federal agencies to undertake activities toward this end. Specifically, the Evidence Act requires agencies to develop Learning Agendas and Annual Evaluation Plans. CISA's evaluations are included in the Department's Annual Evaluation Plans, indicating that the Department has recognized those evaluations as ''significant.'' CISA's SLCGP Evaluation[1] is one such significant evaluation and was included in the Department of Homeland Security FY 2024 Annual Evaluation Plan. CISA SED's Grant Analytics Branch of the Stakeholder Engagement Division and its evaluation services contractor are working together to conduct this study.

CISA SLCGP Evaluation[2]

This evaluation aligns with DHS's FY 2024 Annual Evaluation Plan and is a part of CISA's effort to implement the Evidence Act. This evaluation supports key strategic objectives at both the departmental and agency levels by bringing evidence to bear on relevant decisions including:

- **DHS's Quadrennial Homeland Security Review (2023)**
    - Mission 1: Counter Terrorism and Prevent Threats,
    - Mission 4: Secure cyberspace and Critical Infrastructure,

[1] For consistency with CISA PA&E guidance, the term "mid-term" has been removed from the title of this evaluation in the design report and supporting PRA documents. References to a "mid-term evaluation" may still appear in associated administrative, privacy, and human subjects documentation that were previously submitted and approved. The scope, methods, and timing of the evaluation remain unchanged.

[2] For consistency with CISA PA&E guidance, the term "mid-term" has been removed from the title of this evaluation in the design report and supporting PRA documents. References to a "mid-term evaluation" may still appear in associated administrative, privacy, and human subjects documentation that were previously submitted and approved. The scope, methods, and timing of the evaluation remain unchanged.

    - Mission 5: Build a Resilient Nation and Respond to Incidents, and
    - Mission 6: Combat Crimes of Exploitation and Protect Victims.
- **CISA Strategic Plan (2023-2025)**
    - Goal 1: Cyber Defense - Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

The SLCGP is a federal initiative co-administered by CISA and the Federal Emergency Management Agency (FEMA) that provides critical funding to state, local, and territorial (SLT) governments to strengthen their cybersecurity posture. Established under the Infrastructure Investment and Jobs Act of 2021, the program allocates $1 billion over four years to help these entities develop and implement robust cybersecurity plans, address resource gaps, and enhance their capability to protect against growing cyber threats.

The overarching goal of the SLCGP is to assist SLT governments in managing and reducing systemic cyber risk. Program objectives remain the same throughout the four-year program. The FY 2022-2025 SLCGP Notice of Funding Opportunities (NOFOs) state that each recipient's application must be aligned to an objective:
Applicants are required to submit applications that address at least one of the following program objectives in their applications:

1. Develop and establish appropriate governance structures, including by developing, implementing, or revising Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
2. Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
3. Implement security protections commensurate with risk.

4. Ensure organization personnel are appropriately trained in cybersecurity commensurate with responsibility.

The evaluation will assess the SLCGP's implementation and short- and medium-term outcome achievement. The study will answer evaluation questions originally derived from the FY 2024 DHS Annual Evaluation plan and the program's FY 2024 Evidence Overview, including:

1. How do SLT implementation approaches vary?
2. What SLCGP funded projects are most commonly utilized to mitigate cybersecurity incidents?
3. How have SLT government recipients leveraged new technology and cybersecurity tools to mitigate cybersecurity threats and incidents?
4. What SLCGP funded interventions were most effective at mitigating threats and ensuring continuity of SLT government operations?
5. What barriers, if any, are preventing the entities from utilizing the grant funds?
6. To what extent are SLT grant recipients using the knowledge gained from SLCGP technical assistance and/or products to prevent cybersecurity incidents?
7. To what extent do regular ongoing phishing training, awareness campaigns; and role-based cybersecurity training for SLT government employees contribute to a reduction in cybersecurity incidents?
8. To what extent have the SLCGP funds increased cybersecurity preparedness of SLT governments and resilience of critical infrastructure?

This evaluation will additionally examine how effectively grant funds are being utilized, understand challenges and successes grant recipients have encountered implementing funds to date, and measure progress made towards the program's short- and medium-term outcomes. The evaluation design is informed by an Evaluability Assessment, which determined that the SLCGP is ready for formal evaluation during or after its fourth funding

year (FY 2025). With the program scheduled to conclude its active funding phase in FY 2026 and the final period of performance to conclude in FY 2029, this evaluation is well-timed to determine the program's effectiveness and provide information to support evidence-based decisions about its future.

Ultimately, the evaluation will enable a nuanced understanding of both the processes and effects of the program on grant recipients, thereby determining the success of SLCGP. Study findings will support continuous program improvement and demonstrate program value added.

This is a new information collection. CISA's Stakeholder Engagement Division (SED) Grant Analytics branch will collect information for this evaluation. Information will be collected from SLCGP recipients via a 60-minute online survey; federal staff members from CISA and FEMA via in-depth interviews; along with the potential addition of a focus group with state Chief Information Officers (CIOs) and/or Chief Information Security Officer (CISOs) representing the 55 SLCGP recipients (if additional information is needed). The potential respondent universe consists of 100-200 representatives from 55 SLCGP recipients and 8-25 CISA and FEMA staff working to administer the program within CISA's SED, Cybersecurity Division (CSD), and Integrated Operations Division (IOD), along with FEMA's Grant Programs Directorate (GPD).

Electronic Survey

All state CIOs and/or CISOs, who serve as the head of their state or territory's SLCGP Cybersecurity Planning Committee in the grant year 2025 or thereafter, will receive the survey via email. While the total number (N) of responses for SLCGP recipients is 55 (one survey response per state or territory participating in the SLCGP), the total respondent universe for SLCGP recipients will range from 100-200 contributors. This is due to the ability of each state or territory's CIO/CISO to invite relevant members of their

State Administrative Agencies (SAAs) and/or SLCGP Cybersecurity Planning Committees to collaborate with them in answering the survey questions.

To conduct outreach, a comprehensive contact database will be compiled using official grant recipient information and each response will be linked to a non-personal identifier. To compile this database, CISA SED will provide the evaluation team with a list of state Chief Information Officer (CIO) and Chief Information Security Officer (CISO) names and emails. The survey distribution will follow a clear communication plan, beginning with an initial email notification explaining the evaluation purpose, timeline, and mandatory participation requirements as stipulated in the Notice of Funding Opportunity. Following this introduction, the Qualtrics survey link will be distributed via email to identified stakeholders, with clear instructions, estimated completion time (60 minutes), and technical support contact information. Automatic reminders will be sent to non-respondents at scheduled intervals to maximize response rates. The survey will collect only personal identifying information for contact purposes (first name, last name, locality/entity name, job title, and work email address), with no additional PII from respondents.

SED has designed the survey to gather both quantitative and qualitative feedback from program participants. Questions will align with program objectives and evaluation metrics outlined in recipients' approved Cybersecurity Plans and projects, ensuring relevant data collection. The questions will focus on how the program is being implemented to date. This information will help assess whether program activities are being implemented with fidelity to the program’s logic model and observe the intermediate outcomes of the program as it relates to recipient cyber posture improvement. Questions will additionally focus on any challenges recipients are facing in program fund implementation, as well as what successful strategies that have applied to date.

Federal Staff Interviews

The interviews will gather information from federal staff at CISA (SED, CSD, and IOD) and FEMA (GPD). These virtual interviews, being held on Microsoft Teams, will provide in-depth insights on the program's design intent, policy objectives, and regulatory compliance, while enabling cross-state comparisons and identification of best practices as observed by federal staff. Additionally, federal staff can offer technical expertise, insights into stakeholder relationships, and perspectives on administrative challenges. Some topics will intentionally appear in both the survey and the interviews, as the interviews allow for greater depth and context to complement survey findings. Participation in the interviews is voluntary.

Potential Collection of Information via SLCGP Focus Group Discussions

The survey will provide an option for recipients to opt-in to a voluntary focus group in order to share more context around their responses to the survey questions over a subsequent MS Teams call(s). A post-hoc focus group may be utilized if more contextual evidence is needed to support a robust understanding of recipient responses. However, if survey response data is sufficient in quantity and clarity, this evaluation team will opt not to employ subsequent focus group engagement in an effort to reduce burden. If a focus group is not held, all those who ‘opted in’ to participate will be notified and all opt-in status data collected via the survey will be expunged from the MS SharePoint folder.

If employed, recipients who indicated interest in voluntary participation will be notified via email about the date and time of the focus group, along with a calendar invite sent via email. Depending on the volume of participants, multiple focus group times may be offered to accommodate schedules for maximum attendance. During the session, questions will not deviate from the survey question categories. Participants will be asked

questions aligned with the survey topics to provide more detailed and context-rich responses.

Survey, interview, and focus group findings will be synthesized into a comprehensive report for SED leadership, presenting key insights about program implementation, successful practices, challenges, trends/patterns, and recommendations for improvement for subsequent funding years. Results will be used to inform future program iterations and shape policy developments related to cybersecurity grant management. Relevant findings will be incorporated into required reports to Congress and the Office of Management and Budget (OMB) regarding the program's early outcomes and effectiveness. The collection of information at the midterm stage of program will establish baseline metrics for comparison in future program evaluations, creating a longitudinal view of program performance and demonstrating CISA's commitment to maximizing the impact of the SLCGP on strengthening the nation's cybersecurity infrastructure at state and local levels.

Usability Testing

The survey instrument was tested in a pilot study conducted with a convenience sample of eight representatives from CISA SED, Integrated Operations Division (IOD), FEMA Grant Programs Directorate (GPD), and regional CISA representatives who work hand-in-hand with the target survey population. The purpose of the pilot was to estimate survey burden, assess respondents' understanding of the survey questions, test usability, and identify improvements in the flow and structure of the survey. Results from the question "Did the survey feel burdensome in any way (e.g. too time-consuming, repetitive, unclear questions)?" identified 50 percent of respondents reporting the survey as "somewhat burdensome" due to its length, with 38 percent reporting "no, it was straightforward," and 12 percent reporting "yes, it was frustrating to complete." In response, the evaluation

team reviewed the survey for repetitive or redundant questions, which were subsequently collapsed or removed. Sections within the survey that were similar to each other were also consolidated into a single section to streamline the structure. Additionally, skip logic functions within the survey were maximized in order to reduce survey-taking time. Ultimately, 62 percent of usability testers reported being "extremely confident" that Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) would be able to answer all survey questions. Zero percent of pilot testers reported they were “not confident” that CIOs/CISOs could answer the survey questions.

While the focus group and interview guides were not pilot tested, they were reviewed and approved by CISA’s Program Analysis and Evaluation Branch; CISA’s Office of Privacy, Access, Civil Liberties, and Transparency; and DHS’ Compliance Assurance Program Office. Because they are open-ended semi-structured guides, the focus group and interview facilitators on the evaluation team can rephrase and/or elaborate upon questions until the respondent understands them. Focus group and interview facilitators will be trained to stop at the one-hour mark, so the time burden is already known. Burden reduction is further considered and implemented through the optional nature of the focus groups. If survey response data is sufficient in quantity and clarity, the evaluation team will not employ subsequent focus group engagement.

The evaluation team will not be collecting data from small businesses or small entities, only federal, state, and territorial government staff members.

Without collecting this information, CISA will not meet the requirements of the Evidence Act to conduct program evaluations—particularly, this evaluation, which was included in the Department of Homeland Security FY 2024 Annual Evaluation Plan as a “significant” evaluation. In addition, without collecting this information, SED, other CISA stakeholder

engagement programs, and CISA-at-largecannot determine whether, or to what extent, SLCGP activities, funds, and services deliver value and utility to stakeholders in supporting informed decision-making and risk reduction. Thus, CISA will not have the information needed to learn how to improve the planning, execution, and delivery of the SLCGP funds and services so that they are more meaningful, relevant, timely, and actionable for stakeholders. Without collecting this information, we will also not be able to assess how to best engage and build trusted relationships with stakeholders, which is needed to identify areas for improvement in how CISA collaborates and interacts with stakeholders to support information exchange within and across sectors.

The following privacy notice, obtained from CISA's Office of Privacy, Access, Civil Liberties and Transparency (PACT), will be displayed on the survey landing page:

Privacy Notice:

Authority: Homeland Security Act of 2002, Pub. L. No. 107-296, § 2220A and § 2220A(q)(2) codified as amended at 6 U.S.C. § 665g.

Purpose: The DHS Cybersecurity and Infrastructure Security Agency (CISA) Stakeholder Engagement Division (SED) Grant Analytics Branch will use this information to evaluate quantitative and qualitative feedback regarding the effectiveness of the State and Local Cybersecurity Grant Program (SLCGP) to understand how state, local, and territorial organizations approach cybersecurity planning and implementation.

Routine Use: The information collected will be aggregated for disclosure in its report to DHS Program Analysis & Evaluation (PA&E) and FEMA Grants Programs Directorate (FEMA GPD) as well as within CISA to the program as it relates to enhancing the

security and resilience of critical cyber infrastructure. Relevant findings may also be incorporated into required reports to Congress and the Office of Management and Budget (OMB) regarding the program's early outcomes and effectiveness.

Disclosure: Providing this information is required by the Notice of Funding Opportunity (NOFO). Not providing the requested information may prevent DHS from evaluating the program's progress toward meeting goals and outcomes as outlined in the grant funding. This is a new information collection.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

ANALYSIS:

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

Title: Stakeholder Engagement Division (SED) State and Local Cybersecurity Grant Program (SLCGP) Evaluation[3]

*OMB Number***:** 1670-NEW

*Frequency***:** ONCE

*Affected Public***:** State and Territorial Chief Information Officers and Chief Information Security Officers participating in the SLCGP

*Number of Respondents***: 72**

*Estimated Time Per Respondent***:** 1 hour for 55 respondents (Survey Only) and 1 hour for 17 respondents (Potential Additional Focus Group);

*Total Burden Hours***:** 72

Total Annual Burden Cost: $13,244.34

Total Annual Government Burden Cost: $348,245.61

Winfield P Werntz,
Acting Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2026-10893 Filed: 5/29/2026 8:45 am; Publication Date: 6/1/2026]

[3] For consistency with CISA PA&E guidance, the term "mid-term" has been removed from the title of this evaluation design report. References to a "mid-term evaluation" may still appear in associated administrative, privacy, and human subjects documentation that were previously submitted and approved. The scope, methods, and timing of the evaluation remain unchanged.