



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

FACT SHEET

State and Local Cybersecurity Grant Program Fact Sheet

Fiscal Year (FY) 2025

Publish Date: August 12, 2025

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](/topics/cybersecurity-best-practices)

In Fiscal Year (FY) 2025, the Department of Homeland Security (DHS) is providing \$91.7 million to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, and territorial (SLT) governments.

Overview

Our nation faces unprecedented threats to the homeland from increasingly sophisticated criminal groups and nation-state actors. State, local, and territorial (SLT) entities stand at the forefront of cyber defense. This partnership includes enforcing laws, assisting the federal government in securing cyberspace, and dismantling transnational criminal

organizations. Cybersecurity threats, including ransomware intrusions, and widespread software vulnerabilities affecting SLT systems and critical infrastructure are increasingly exploited by malicious actors, operating both domestically and abroad.



Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of SLT governments is the focus of the State and Local Cybersecurity Grants Program (SLCGP). Through funding from the Infrastructure Investment and Jobs Act, the SLCGP enables DHS to make targeted cybersecurity investments that strengthen the security and resilience of critical infrastructure and our SLT partners from cyberattacks.

The SLCGP is being jointly managed by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA). CISA will provide subject-matter expertise and determine allowable activities, and FEMA will conduct eligibility reviews and administer the grant awards consistent with all applicable laws, regulations, and policies.

Goals and Objectives

CISA and FEMA developed a series of goals and objectives for the SLCGP based on input from state, local, and territorial stakeholders, and consideration of national priorities, frameworks, and the national cyber threat environment:

1. Implement cyber governance and planning;
2. Assess and evaluate systems and capabilities;
3. Mitigate prioritized issues; and
4. Build a cybersecurity workforce.

Applicants who have completed and received approval of their initial requirements under Objective 1 can pursue any of the four program objectives in FY 2025. In FY 2025, applicants should continue to build from their previous projects submitted in previous fiscal years in accordance with their Cybersecurity Plan.

Funding

In FY 2025, \$91.7 million is available for awards under the SLCGP. Each state and territory will receive a funding allocation as determined by the statutory formula. Allocations for states and territories include a base level as defined for each entity: 1% for each state, the District of Columbia, and the Commonwealth of Puerto Rico; and 0.25% for American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands. State allocations include additional funds based on a combination of state and rural population totals. 80% of total state or territory allocations must support local entities, while 25% of the total state or territory allocations must support rural entities.

Eligibility

All 56 states and territories, including any state of the United States, the District of Columbia, Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the U.S. Virgin Islands, are eligible to apply for SLCGP funds. To be eligible to receive FY 2025 SLCGP funding, states and territories must have fulfilled the initial SLCGP requirements of developing a CISA-approved Cybersecurity Plan, Cybersecurity Planning Committee List, and Charter. The Governor-designated SLCGP State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS/FEMA.

Funding Guidelines

Cybersecurity Planning Committee and Cybersecurity Plan

Cybersecurity Planning Committees are charged with coordinating, developing, and approving the entity's Cybersecurity Plan. Eligible entities were required to submit Cybersecurity Plans for review and approval as part of their FY 2022 grant application. Additionally, plans are treated as living documents that can be resubmitted and updated as appropriate and can receive CISA regional staff support as needed.

All entities with a CISA-approved Cybersecurity Plan must submit their current plan to CISA via the FEMA SLCGP Inbox (FEMA-SLCGP@fema.dhs.gov) no later than **January 30, 2026**, in accordance with the annual resubmission requirement. When they submit, entities must indicate if the plan has been revised since CISA's approval. If it has been revised, they must provide a brief explanation of any revisions.

There is no requirement for an entity to revise their CISA-approved Cybersecurity Plan unless CISA notifies them that it does not meet plan requirements.

Cybersecurity Best Practices and Performance Measures

Entities must clearly articulate efforts to implement the [Key Cybersecurity Best Practices](https://www.cisa.gov/cybergrants/slcgp#:~:text=key%20requirement%3a%20building.gov%20internet%20domain) for Individual Projects as listed in the FY 2025 Notice of Funding Opportunity (NOFO). These efforts should be documented in their Cybersecurity Plan and should be prioritized in the individual projects the entity pursues. The assessment and evaluation activities described in Objective 2 of the program can be used to measure the successes and failures of adopted Key Cybersecurity Best Practices as outlined in the Cybersecurity Plan.

Performance measures are data used to gauge program performance. The FY 2025 NOFO contains a list of performance measures, some of which overlap with the best practices, that applicants are encouraged to consider when evaluating their program performance.

Conferring with these measures will help applicants ensure their projects are meeting CISA standards for improving cybersecurity posture.

Pass-through Requirements

The SLCGP SAA recipient must pass-through at least 80% of its awarded funds to local units of government, including at least 25% of its awarded funds to rural areas of the state or territory. The pass-through to rural entities is part of the overall 80% pass-through requirement to local governments. All pass-through entities must meet all program and grant administration requirements. See *2 CFR § 200.332* <<https://www.ecfr.gov/current/title-2/subtitle-a/chapter-ii/part-200/subpart-d/subject-group-ecfr031321e29ac5bbd/section-200.332>>. For a description of eligible subrecipients, please see Section 2.A.b. of the FY 2025 SLCGP NOFO.

FEMA interprets the date that an entity “receives a grant” to be the date upon which FEMA releases the funding hold in the [FEMA Grants Outcomes \(FEMA GO\) system](https://go.fema.gov/login) <<https://go.fema.gov/login>>. Therefore, the 45-day pass-through requirement starts on the date when the amendment is issued in the FEMA GO system and FEMA makes the funding available to the SLCGP SAA for drawdown. After the funds have been released, FY 2025 SLCGP recipients must submit a letter to FEMA signed by the Authorized Official listed in the grant award certifying that they have met the 45-day pass-through requirement and collected any signed local government consents. Local consents must be signed by the Authorized Official for the local government entity receiving the items, services, capabilities, or activities in lieu of funding, and the consent must specify the amount and intended use of the funds. This letter is due no later than 10 calendar days after the 45-day period for issuing pass-through funding has passed. The letter should be emailed to FEMA-SLCGP@fema.dhs.gov. FEMA will send a copy of the letter to CISA.

Pass-through is defined as an obligation on the part of the entity or multi-entity group to make funds available to local units of government, combinations of local units, tribal governments, or other groups or organizations; not necessarily the full funding passed

within that 45-day window. With the consent of the local government, the pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. Four requirements must be met to pass-through grant funds:

- The SAA must make a firm written commitment to passing through grant funds or equivalent services to local government subrecipients;
- The SAA's commitment must be unconditional (i.e., no contingencies for the availability of SAA funds);
- There must be documentary evidence (e.g., subgrant award document with terms and conditions) of the commitment; and
- The award terms must be communicated to the subrecipient.

Cost Share Requirements

Eligible entities must meet a 40% cost share requirement for the FY 2025 SLCGP, except for multi-entity projects which require a 30% cost share. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants must agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 40% of the total project costs (federal award amount plus cost share amount, rounded up to the nearest whole dollar). Consistent with previous fiscal years and in accordance with 48 U.S.C. §1469a, cost share requirements for FY 2025 are waived for the following entities: American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

Cost share waivers will not be considered for any entities in FY 2025 SLCGP. Also, unless otherwise authorized by law, federal funds cannot be matched with other federal funds. The recipient's contribution should be specifically identified. These non-federal contributions have the same eligibility requirements as the federal share.

Multi-Entity Projects

Multiple eligible entities (states or territories) can group together to address shared cybersecurity risks and threats to information systems within the eligible entities' jurisdictions (including local governments and rural jurisdictions). There is no separate funding for multi-entity projects. Instead, these investments would be considered as group projects: each group member contributes an agreed-upon funding amount from their SLCGP award to the overall project. Each group member's financial contribution is then funded from their individual SLCGP award. Each participating state or territory in the group should include the multi-entity project in their individual Investment Justification (IJ) and Project Worksheet (PW) submissions with their application. It is expected that IJs and PWs for multi-entity projects will be almost identical. Any differences should be as a result of alignment with each group member's respective Cybersecurity Plan.

Timing: Even though applications from each State and/or Territory that are part of the multi-entity project may come in at different times, FEMA and CISA will need to approve the multi-entity projects in each separate application at the same time. This is because, unless both states and/or territories complete their respective responsibilities in the multi-entity project, then the project would not be successful. As a result, FEMA and CISA will not award one state's/territory's portion of the multi-entity project in isolation without approving the other.

Nature of a Multi-Entity Project: The states and/or territories must work together to implement each other's cybersecurity plans to address cybersecurity risk and cybersecurity threats to their information systems in order to have a multi-entity project. If one state or territory can accomplish the scope of work under a project without any need to work with the other state and/or territory, then it is not a multi-entity project.

Cooperating Purchasing. To foster greater economy and efficiency, two or more states may conduct joint procurement or pursue some other type of cooperative purchasing arrangement to procure equipment, supplies, or services. Such a collaborative procurement action does not mean that the states are pursuing a multi-entity project.

Rather, it is the substance of the underlying scope of work that makes a project a multi-entity project and not the manner in which a state is procuring services in accomplishing a project's scope of work.

Examples. The following examples help illustrate the considerations above.

- Example 1: State X and Y seek to jointly conduct cybersecurity training of their state personnel. Rather than each state conducting its own \$250K worth of training for their respective employees, they want to work together to have joint training sessions so that all trainees get \$500K worth of training. There will be ten training sessions for all state X and Y employees and each state will be responsible for organizing and executing five sessions. The states, furthermore, jointly conduct a procurement to obtain a contractor that will provide services to help the state carry out all ten sessions. This would be a multi-entity project because both states have to work together to carry out the scope of work, each state is implementing the cybersecurity plan of each other's by training the other state's employees, and there is a shared project objective.
- Example 2: State X and Y seek to conduct cybersecurity training for their own staffs. To obtain greater cost-savings, the states jointly procure a contractor to conduct their cybersecurity training. Following the procurement, each state runs their own training program and uses the same contractor in doing so. This is not a multi-entity project. This is because each state could accomplish their respective project without working together with the other state to carry out the scope of work, one state is not implementing the cybersecurity plan of the other state by carrying out activities to reduce cybersecurity threats and cybersecurity risks to the other state's information systems, and there is no shared project objective.

Management and Administrative Costs

Management and Administrative (M&A) Costs are allowed. A maximum of up to 5% of SLCGP federal funds (federal award amount plus cost share amount, not rounded up to the nearest whole dollars) may be retained by the SAA, and any funds retained are to be used solely for M&A purposes associated with the SLCGP award. Subrecipients (state agencies or local units of government) may also retain a maximum of up to 5% of the federal funding passed through by the state solely for M&A purposes associated with the SLCGP award. While the

eligible entity may retain up to 5% of this total for M&A, the state must still ensure that all subrecipient award amounts meet the mandatory minimum pass-through requirements that are applicable to SLCGP. To meet this requirement, the percentage of funds passed through to local governments must be based on the state's total SLCGP award prior to withholding any M&A.

Application Process

Applying for an award under the SLCGP is a multi-step process. Applicants are encouraged to register early in the System for Award Management ([SAM.gov](https://sam.gov/content/home) <https://sam.gov/content/home>) and the [FEMA GO](#) system, as the registration process can take four weeks or more to complete. Registration should be done in sufficient time to ensure it does not impact a state or territory's ability to meet required submission deadlines. Section 5: Submission Requirements and Deadlines in the FY 2025 SLCGP NOFO contains more detailed information and instructions.

All application materials will be posted on [Grants.gov](https://www.grants.gov/) <https://www.grants.gov/> and the [FEMA SLCGP Website](https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program/fy-24-nofo). <https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program/fy-24-nofo> Eligible applicants must submit their application through the [FEMA GO](#) system. Applicants needing technical support with FEMA GO should contact FEMAGO@fema.dhs.gov or call the FEMA GO Help Desk at 1-877-585-3242, Monday – Friday from 9 a.m. – 6 p.m. ET.

Completed applications must be submitted in the FEMA GO system no later than 5 p.m. ET on August 15, 2025.

Period of Performance Extension Requests

Extensions to the FY 2025 period of performance for this program are not allowed.

SLCGP Resources

There are a variety of resources available to address programmatic, technical, and financial questions, which can assist with SLCGP applications:

- The FY 2025 SLCGP funding notice is located online at [grants.gov](https://grants.gov/search-results-detail/360215) <<https://grants.gov/search-results-detail/360215>>.
- For additional program-specific information, please email FEMA-SLCGP@fema.dhs.gov. Applicants may also contact their FEMA preparedness officer.
- For support regarding financial grants management and budgetary technical assistance, applicants may contact the FEMA Award Administration Help Desk, via e-mail at ASK-GMD@fema.dhs.gov.
- For support regarding programmatic elements, applicants may contact CISA via e-mail at SLCGPinfo@mail.cisa.dhs.gov. SLTs can reach out to their CISA Regional Staff. For regional contact information, please visit [cisa.gov/about/regions](https://www.cisa.gov/about/regions) <<https://www.cisa.gov/about/regions>>.

Existing ZoomGrants™ Users: Email

skinnear@cc

Password

.....

☐ Stay logged in? (Admins and Reviewers only)

Login

Forgot password?

HELP

RESOURCES

A▲▼

You must be logged in to apply.

New ZoomGrants™ Account

Wyoming Office of Homeland Security

State and Local Cybersecurity Grant Program

(SLCGP)

Deadline 5/15/2026

VIEW OPEN PROGRAMS

|

HIDE SLCGP GRANT DESCRIPTION

HIDE REQUIREMENTS

SHOW LIBRARY

SHOW CONTACT ADMIN

SLCGP Grant Description [\[hide this\]](#)

The DHS/FEMA State and Local Cybersecurity Grant Program (SLCGP) is administered by the Wyoming Office of Homeland Security (WOHS) as the State Administrative Agency (SAA). The goal of SLCGP is to assist state, local, and tribal (SLT) governments with managing and reducing systemic cyber risk.

WOHS is required to ensure that at least 80% of SLCGP funding is passed-through to local governments, with at least 25% of the funding allocated to rural areas. This pass-through can be done via direct applications from local governments or by passing through items, services, capabilities, or activities to local governments in lieu of funding.

SLCGP projects must address one of the following objectives:

- Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Objective 2: Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Objective 3: Implement security protections commensurate with risk.
- Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Requirements [\[hide this\]](#)

Eligible applicants must be a state, local, tribal or other unit of local government (Hospital/School/Water District, Public Higher Education, etc).

All successful SLCGP applicants must have a valid Unique Entity Identifier (UEI) from SAM.gov at the time of award.

A separate ZoomGrants application must be submitted for each project you are seeking funding for.

All questions in this ZoomGrants application must be completed.

Applications must include quotes, or other documentation, to support the requested amount.

Application Status: Not Submitted

\$ 0.00 requested

You must be logged in to begin.

Summary

Application Questions

Budget

Documents

Activity Log

Application Questions

(answers are saved automatically when you move to another field)

1. Organization Type

- ☐ State Government
- ☐ County Government
- ☐ City/Town Government
- ☐ Tribal Government
- ☐ School District
- ☐ Hospital District
- ☐ Institution of Higher Education
- ☐ Other Special District
- ☐ Other

2. What cybersecurity framework does your organization subscribe to and how far along are you in implementing that framework?

Maximum characters: 65000. You have characters left.

3. Please briefly describe the cybersecurity project.

Maximum characters: 65000. You have characters left.

4. SLCGP projects must align with one of the 4 following objectives. Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations. Objective 2: Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments. Objective 3: Implement security protections commensurate with risk. Objective 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Which objective does the project align with?

- ☐ Objective 1
- ☐ Objective 2
- ☐ Objective 3
- ☐ Objective 4

5. How does the project impact or support your jurisdiction's cybersecurity efforts?

Maximum characters: 65000. You have characters left.

6. Does the project protect critical infrastructure? If so, please describe the infrastructure and how this project will impact it.

Maximum characters: 65000. You have characters left.

7. Continued federal funding and ongoing support is not guaranteed. Do you have local support and/or funding to continue the project beyond the federal funding should it be awarded?

Maximum characters: 65000. You have characters left.

8. Will you accept partial funding?

Maximum characters: 65000. You have characters left.

9. What date do you anticipate the project to be completed?

Maximum characters: 65000. You have characters left.

10. Please submit a minimum of three (3) milestones associated with this project.

Maximum characters: 65000. You have characters left.

11. I understand that this is a competitive grant program and that submitting this application does not guarantee funding. The Wyoming Cybersecurity Planning Committee will review applications and make funding determinations. If selected for funding, the Wyoming Office of Homeland Security will contact you to discuss next steps.

- ☐ Yes
- ☐ No

Previous

Next

Application ID: -1