FY 2023 State and Local Cybersecurity Grant Program Fact Sheet

In Fiscal Year (FY) 2023, through the Infrastructure Investment and Jobs Act, the Department of Homeland Security (DHS) is providing approximately $375 million to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, and territorial governments.

OVERVIEW

The goal of the State and Local Cybersecurity Grant Program (SLCGP) is to help states, local governments, rural areas, tribes, and territories address cybersecurity risks and cybersecurity threats to information systems. The program enables DHS to make targeted cybersecurity investments in state, local, and territorial government agencies, thus improving the security of critical infrastructure and resilience of the services that those entities provide to their communities. Federally recognized tribes also have a dedicated grant program; details on the Tribal Cybersecurity Grant Program can be found at cisa.gov/Tribal-Cybersecurity-Grant-Program. The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA) are jointly managing the SLCGP. CISA will provide subject-matter expertise and determine allowable activities, while FEMA will conduct eligibility reviews, and issue/administer the grant awards consistent with all applicable laws, regulations, and policies.

GOALS AND OBJECTIVES

CISA and FEMA developed a series of overarching 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.

In FY 2023, applicants who have completed and received approval of their FY 2022 requirements surrounding Objective 1 will shift focus toward the next objectives. In particular, applicants will work towards Objectives 2 and 3 of the program to begin assessment planning efforts and implement security protections.

FUNDING

In FY 2023, $374.9 million is available under the SLCGP, with varying funding amounts allocated over four years from the Infrastructure Investment and Jobs Act. This year, each state and territory will receive a funding allocation as determined by the statutory formula:

- Allocations for states and territories include a base funding level as defined for each entity: 1% for each state, the District of Columbia, and 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 population and rural population totals.
- 80% of total state allocations must support local entities, while 25% of the total state allocations must support rural entities; these amounts may overlap.

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 2023 SLCGP funding, states and territories must have fulfilled the FY 2022 SLCGP requirements of a CISA-approved Cybersecurity Plan, Cybersecurity Planning Committee List, and Charter. The designated State Administrative Agency (SAA) for each state and territory is the only entity eligible to apply for SLCGP funding.

FUNDING GUIDELINES

Cybersecurity Planning Committee and Cybersecurity Plan Requirements

In FY 2022, each state and territory was required to establish a Cybersecurity Planning Committee that coordinates, develops, and approves a Cybersecurity Plan. These plans are meant to guide development of cybersecurity capabilities across the state or territory. The Cybersecurity Planning Committee is responsible for approving the Cybersecurity Plan and prioritizing individual projects. Eligible entities were required to submit Cybersecurity Plans for review and approval as part of their FY 2022 grant application. Initial Cybersecurity Plans will be approved for two years and subsequent Cybersecurity Plans, building on the investments from the previous year(s), must be submitted for approval annually beginning in FY 2024.

For FY 2023, there are no new Cybersecurity Planning Committee or Cybersecurity Plan requirement. CISA considers Cybersecurity Plans as living, strategic documents. States and territories have the option to resubmit and update their Cybersecurity Plan, with the continued support of CISA regional staff, if needed.

NEW: Assessment, Evaluations, and Cybersecurity Best Practices Requirements

Each applicant must adopt key Cybersecurity Best Practices as required during the creation of the Cybersecurity Plan and within individual projects. The assessment and evaluation activities described in Objective 2 of the program are meant to measure the successes and failures of adopted Cybersecurity Best Practices as outlined in the Cybersecurity Plan. In addition, the Cybersecurity Best Practices should consult the Cybersecurity Performance Goals (CPGs) to ensure a strong 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 C.F.R. § 200.332*. For a description of eligible subrecipients, please see Section C.1.b. of the FY 2023 SLCGP Notice of Funding Opportunity (NOFO).

FEMA interprets the date that an entity "receives a grant" to be the date upon which FEMA releases the funding hold in the Non-Disaster (ND) Grants system. Therefore, the 45-day pass-through requirement starts on the date when the amendment is issued in the ND Grants System releasing the funding hold and FEMA makes the funding available to the SLCGP SAA for drawdown. After the funds have been released, FY 2023 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 specific groups or organizations; not necessarily the full funding passed within that 45-day window. 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.

Multi-Entity Groups

An SAA may partner with other SAAs to form a multi-entity group. Members of these groups work together to address cybersecurity risks and cybersecurity threats to information systems within their jurisdictions. There is no limit to the number of participating entities in a multi-entity group. Local entities can be included in the project, but their respective eligible entity (i.e., the SAA) must also participate at some level. There is no separate funding for multi-entity awards. Instead, they should be considered as group projects within their existing state or territory allocations. These projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Cybersecurity Planning Committee and be aligned with each respective eligible entity's Cybersecurity Plan.

Cost Share Requirements

Eligible entities applying as a single entity must meet a 20% non-federal cost share requirement for the FY 2023 SLCGP except for Multi-Entity Projects which require a 10% cost share. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). In other words, the federal share applied toward the SLCGP budget at the project/activity level shall not exceed 80% of the total budget as submitted in the application and approved in the award. If the total project ends up costing more, the recipient is responsible for any additional costs.

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.

The Secretary of Homeland Security may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. Additionally, the Secretary has issued a blanket waiver of cost share requirements for the insular areas of the U.S. territories of Puerto Rico, American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. More information on what constitutes economic hardship, and how to request a cost share waiver will be forthcoming.

For a multi-entity group project, a cost share is 10% for the FY 2023 SLCGP.

APPLICATION PROCESS

Applying for an award under the SLCGP is a multi-step process. Applicants are encouraged to register early 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 D in the FY 2023 SLCGP Notice of Funding Opportunity contains more detailed information and instructions.

Eligible applicants must submit their initial application through the portal at www.grants.gov. Applicants needing grants.gov support should contact the customer support hotline at (800) 518-4726, 24 hours per day, 7 days per week except federal holidays.

Eligible applicants will be notified by FEMA and asked to proceed with submitting their complete application package in the Non-Disaster (ND) Grants System. Applicants needing technical support with the ND Grants System should contact ndgrants@fema.dhs.gov or (800) 865-4076, Monday-Friday from 9 a.m. to 6 p.m. Eastern Time (ET).

Completed applications must be submitted no later than 5 p.m. ET by the deadline included in the funding notice.

SLCGP RESOURCES

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

- The SLCGP funding notice will be released no later than July 11, 2023, and available online at www.fema.gov/grants and www.grants.gov.
- For additional support and guidance, SLTTs should reach out to their CISA Regional Staff. For contact information for your region, please visit cisa.gov/about/regions.
- For additional program-specific information regarding programmatical elements, applicants may contact CISA via e-mail at SLCGPinfo@cisa.dhs.gov.
- For additional program-specific information regarding funding and budgetary technical assistance, applicants may contact FEMA via e-mail at FEMA-SLCGP@fema.dhs.gov.