STATE AND LOCAL

CYBERSECURITY GRANT PROGRAM

FREQUENTLY ASKED QUESTIONS

BACKGROUND

In the Bipartisan Infrastructure Law, also known as the Infrastructure Investment and Jobs Act (IIJA), Congress established the State and Local Cybersecurity Grant Program (SLCGP) to "award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments." Within the U.S. Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA) are implementing this authority through two grant programs:

1. The SLCGP, which allows state and territory State Administrative Agencies (SAAs) to apply for grant funding. Under SLCGP, states and territories are the only eligible entities. Local and tribal governments are eligible subrecipients under this program.
2. The Tribal Cybersecurity Grant Program (TCGP), which allows Tribal governments to apply for grant funding. Under TCGP, Tribal governments of federally-recognized Tribes are the only eligible entities and do not apply for funding through SAAs.

This FAQ addresses common questions about the SLCGP. Additional information on the TCGP is forthcoming.

GENERAL PROGRAM QUESTIONS

What is the purpose of the SLCGP?

The SLCGP provides funding to state, local, tribal, and territorial (SLTT) governments to address cybersecurity risks and cybersecurity threats to SLTT-owned or operated information systems. All requirements and program guidance are established in the Notice of Funding Opportunity (NOFO).

How much funding is available?

For FY 2022, Congress appropriated $200 million. This includes $185 million for SLCGP, $6 million for TCGP, $8.5 million for DHS to administer the grant, and $500,000 for the DHS Inspector General to evaluate the grant programs. Congress also authorized for appropriation $400 million for FY 2023, $300 million for FY 2024, and $100 million for FY 2025.

How will funds be allocated?

The allocation formula in the Bipartisan Infrastructure Law includes a base level of funding for each state and territory. Allocations for states, the District of Columbia, and Puerto Rico include additional funds based on a combination of total population and rural population. Final FY 2022 SLCGP allocations for each state and territory will be included in the NOFO.

Who is eligible to apply?

The SAAs for states and territories are the only eligible applicants. In addition, two or more eligible entities may apply jointly for assistance as a multi-entity group. Under SLCGP, that means two or more SAAs may apply for joint projects, but they still must submit separate applications.

What is the role of the State Administrative Agency?

The SAA is responsible for managing the grant application and award. Working with the Cybersecurity Planning Committee, the SAA must ensure at least 80% of the federal funds awarded under the SLCGP are passed-through to local entites. In addition, at least 25% of the total funds made available under the grant must be

passed through to rural communities. Receipt of funds occurs when the SAA accepts the award or 15 calendar days after the entity receives notice of the award, whichever comes first.

What are the goal and objectives of the program?
The overarching goal of the program is to assist SLTT governments in managing and reducing systemic cyber risks. To accomplish this, CISA has established four discrete, but interrelated objectives:

- Governance and Planning: Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Assessment and Evaluation: Identify areas for improvement in SLTT cybersecurity posture based on continuous testing, evaluation, and structured assessments.
- Mitigation: Implement security protections commensurate with risk (outcomes of Objectives 1 and 2), using the best practices as described in element 5 of the required 16 elements of the cybersecurity plans and those further listed in the NOFO.
- Workforce Development: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

What are the priorities of the program in the first year?
In the first year, the focus is on establishing a strong foundation on which to build a sustainable cybersecurity program. Initial priorities include the following, all of which are statutory conditions for receiving a grant:

- Establish a Cybersecurity Planning Committee that can lead entity-wide efforts.
- Develop a Cybersecurity Plan that addresses the entire jurisdiction and incorporates cybersecurity best practices.
- Conduct assessments and evaluations to identify gaps that can be mitigated by individual projects throughout the life of the grant program.

Will the grant-funded projects be required to be tied to the Threat and Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR) process?
No. Applicants are encouraged to leverage the THIRA/SPR process, but it is not a requirement.

How long is the period of performance?
The period of performance for each grant year will be 48 months. Extensions are allowed on a case-by-case basis.

How will proposed projects be evaluated?
DHS/FEMA will evaluate applications for completeness and applicant eligibility. DHS/CISA will evaluate applications for adherence to programmatic guidelines and anticipated effectiveness of the proposed investments. The review will include verification of the following elements:

- Establishment of and composition of the Planning Committee;
- Cybersecurity Plan(s) or request for exception;
- Proposed projects that are consistent with the Cybersecurity Plan(s), or will be consistent with the Cybersecurity Plan if requesting a grant to develop a Plan, and SLCGP program objectives and requirements;
- Proposed projects are feasible and effective as reducing the risks the project was designed to address; and
- Proposed projects will be completed within the period of performance.

Additional details on project evaluation criteria are available on page 28 of the NOFO.

LOCAL GOVERNMENTS

How do local governments apply?
Local governments are eligible as subapplicants to their SAA and must work with their state or territory's Cybersecurity Planning Committee to receive subawards.

How are local governments defined?
Local governments are defined in the law as a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity.

How are rural areas defined?
In the law, rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.

What percentage of the funds must be passed through to local entities?
A minimum of 80% of state allocations must be passed through to local governments. In addition, at least 25% of the total funds made available under the grant must be passed through to rural communities. A maximum of 20% can be used by state agencies to administer the grant program.

This pass-through requirement does not apply to the District of Columbia or the U.S. territories. Additionally, this pass-through requirement does not apply to a grant awarded solely to support activities that are integral to the development or revision of the Cybersecurity Plan of the state.

Can the 80% passthrough be in the form of services/solutions procured, managed, and deployed by the state in coordination with the local government benefited?
SAAs can pass through items, services, capabilities, or activities instead of funds with the consent of local governments, but must pass through a minimum of 80% of the value of the award. This same requirement applies to the 25% that must be passed through to rural areas. Pass-through must occur within 45 calendar days of receipt of funds. Receipt of funds occurs when the SAA accepts the award or 15 calendar days after the entity receives notice of the award, whichever comes first.

What is the process for selecting which local governments and rural areas will get funds and for which projects?
Cybersecurity Planning Committees must work collaboratively across the state to identify and prioritize individual projects that align with the state's Cybersecurity Plan. Ultimately, it is up to the state to determine where and how to pass-through funds, with the permission of applicable local governments if passing through items or services in lieu of funding.

COST SHARE

What is the required cost share for individual projects?
For applications made by an individual eligible entity, the FY 2022 non-federal cost-share requirement is 10%.

What is the cost share for a multi-entity project?
There is no cost-share requirement for multi-entity projects in FY 2022.

How does the cost share work?

For FY 2022, the federal share of *any activity* cannot exceed 90% (unless the recipient is a multi-entity group). For example, if a local entity estimates the total cost of a project is $100,000, the local entity's cost share will be 10% or $10,000. The cost share must be at the activity (i.e., project) level. The cost share cannot be shared across multiple projects being implemented by the same entity.

Is there a cost-share waiver?
The Secretary of Homeland Security, or designee, may waive or modify the non-federal share if an eligible entity demonstrates economic hardship. All waiver requests will be considered on a case-by-case basis.

There are a number of factors in determining an economic hardship. An entity that applies for a cost-share waiver must meet at least one of the following six criteria in order to be considered:

- Changes in rates of unemployment in the jurisdiction from previous years;
- Changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. § 2011 et seq.) from previous years;
- Demonstration of fiscal distress that could be caused by changes to statewide budgets already approved prior to knowledge of the SLCGP cost share requirement;
- Demonstration that the rate of unemployment has exceeded the annual national average rate of unemployment for three of the past five years;
- Demonstration that the entity has filed for bankruptcy or been placed under third-party financial oversight or receivership within the past three years; and
- For local units of government only, demonstration that those localities have areas within them that are designated as either "high" or "very high" on the Centers for Disease Control and Prevention's Social Vulnerability Index.

Eligible entities that would like to request a cost-share waiver based on economic hardship should submit a waiver request with their FY 2022 SLCGP application submission in ND Grants with the following information in a written narrative:

- The entity's background/history of economic hardship.
- Any austerity measure(s) the entity has taken to address economic hardship.
- A description of how the lack of a waiver will impact the entity's ability to develop, implement, or revise a Cybersecurity Plan or address imminent cybersecurity threats.
- A detailed justification explaining why the state (or specific local government(s) or specific project(s) if requesting only a partial waiver) is unable to fulfill the cost share requirement. The applicant must identify specific economic hardship(s) and address the factors listed above.

CYBERSECURITY PLANNING COMMITTEE

What are the membership requirements for the Cybersecurity Planning Committee?
The Cybersecurity Planning Committee must include representation from each of the following:

- The eligible entity;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or equivalent official of the eligible entity;
- If the eligible entity is a state, then representatives from counties, cities and towns within the jurisdiction of the eligible entity;
- Public education institutions within the jurisdiction of the eligible entity;
- Public health institutions within the jurisdiction of the eligible entity; and
- As appropriate, representatives of rural, suburban, and high population jurisdictions.

At least half of the representatives of the Cybersecurity Planning Committee must have professional experience in cybersecurity or information technology.

Consideration should be given to include other members, including but not limited to representatives from:

- State and county judicial entities;
- State legislature;
- Election infrastructure officials, including secretaries of state and election directors;
- Representatives from state, territorial, and local public safety, homeland security, emergency management and law enforcement agencies;
- Emergency communications officials;
- City and county CIOs and CISOs;
- Publicly owned or operated critical infrastructure;
- State National Guard if such entities have a cybersecurity mission;
- Municipal, city, county, rural area or other local government councils or associations; and
- Other entities with expertise and skillsets that best represent the cybersecurity interests across the eligible entity.

In addition, the eligible entity must consult its CIO, CISO or equivalent official in allocating funds under an SLCGP grant.

Can existing committees be used?
Yes, existing committees can be used but must follow this guidance:

- An existing multi-jurisdictional planning committee must meet the membership requirements or be capable of being expanded to meet the requirements of the Cybersecurity Planning Committee.
- Membership should reflect an eligible entity's unique cybersecurity risk profile.
- Eligible entities should consider using Senior Advisory Committees or create a subcommittee, modified to meet the membership requirements.

What are the responsibilities of the planning committee?
The responsibilities of the Cybersecurity Planning Committee include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Assisting the state in ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities or activities provided by the eligible entity through this program.

How should planning committees prioritize individual projects?
Individual projects must help achieve the goal and objectives of the entity's Cybersecurity Plan. To prioritize projects, the committee should:

- Coordinate activities across preparedness disciplines and levels of government, including SLTT governments;
- Devise a cohesive planning framework;
- Incorporate CISA and FEMA resources as well as those from other federal and SLTT entities, the private sector, and faith-based community organizations; and

- Determine how available preparedness funding sources can effectively support a whole community approach to emergency preparedness and management and the enhancement of core capabilities.

Can the same planning committee designated for state-level awards be used for multi-entity grants?
There should not be a separate committee or plan for multi-entity activities. Each member of the multi-entity group must have and use their respective Cybersecurity Planning Committee for multi-entity activities and should not have a separate committee that is used solely for multi-entity activities. All SLCGP projects must be reviewed and approved by each entity's committee. All multi-entity projects must be tied to the respective Cybersecurity Plan for each entity.

CYBERSECURITY PLANS

Who is required to submit a Cybersecurity Plan?
States and territories must submit Cybersecurity Plans for review and approval as part of their grant applications. If your entity is applying for grant funds to develop a Cybersecurity Plan, the plan is not required to be submitted as part of the FY 2022 application, but must be submitted for DHS review and approval by September 30, 2023.

Who must approve the Cybersecurity Plan before it is submitted to DHS?
The Cybersecurity Planning Committee and the CIO, CISO or equivalent official must approve the Cybersecurity Plan and individual projects before submitting to DHS.

How often am I required to submit a Cybersecurity Plan?
Initial Cybersecurity Plans will be approved for two years. Subsequent Cybersecurity Plans, building on the investments from the previous year(s), must be submitted for approval annually.

Are there specific requirements for the Cybersecurity Plan?
The Cybersecurity Plan should establish high level goals and finite objectives to reduce specific cybersecurity risks across the eligible entity. The Cybersecurity Plan should also serve as the overarching framework for the achievement of the SLCGP goal, with grant-funded projects working to achieve outcomes. Regional approaches, as part of an entity-wide approach, should also be considered.

In developing the Cybersecurity Plan, the Cybersecurity Planning Committee should consider the following:

- Existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;
- Existing assessments and evaluations (e.g., reports, after action reports) conducted by SLTT governments within the entity and any planning gaps that require additional assessments and/or evaluations; and
- Identification of potential SLCGP projects to address planning gaps and prioritize mitigation efforts.

The full list of requirements for the Cybersecurity Plan are available in Appendix C of the NOFO.

Are local governments required to produce their own Cybersecurity Plan?
No. Local governments will be part of the eligible entity's Cybersecurity Plan. These plans are meant to guide development of cybersecurity capabilities across the state or territory. The plans are not meant to be agency specific.

Can funds be used to sustain or expand existing efforts?
Yes. If existing efforts involve improvements made to cyber systems and meet the required elements, and as long as those funds are not used to supplant state or local funds, then grant funds can be used to continue or

expand those existing efforts. The awards must meet the goal of the program, which is to manage and reduce systemic cyber risk to SLTT information systems. The projects should achieve a sustainable improvement solution that will remain even after the expiration of the cybersecurity grant program. The ultimate goal of the program as stated in the legislation will be to award grants to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, SLTT governments.

Can existing plans be used?
Eligible entities are encouraged to incorporate, where applicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local and territorial entities.

Does DHS approve the submitted Cybersecurity Plans?
Yes. Once approved by the Cybersecurity Planning Committee, CIO, and CISO or equivalent official, CISA and FEMA will review each submitted Cybersecurity Plan. CISA will approve the final Cybersecurity Plans.

Is there a template or guidance for the Cybersecurity Plan and individual projects?
Yes. CISA offers a downloadable cybersecurity plan template. This template may be used by states and locals, or may be referenced as necessary. The template is located on the CISA.gov website.

Is there a timeline that the Cybersecurity Plan must cover?
The plan is strategic in nature and recommended that it address a two-to-three-year period.

MULTI-ENTITY PROJECTS

What are multi-entity projects and who can apply?
Multiple eligible entities (i.e., states or territories) can group together to address cybersecurity risks and threats to information systems within the eligible entities' jurisdictions.

Are there additional requirements for multi-entity projects?
Yes. In addition to each eligible entity having a Cybersecurity Plan approved by CISA and an established Cybersecurity Planning Committee, multi-entity groups must also have a multi-entity Investment Justification for the proposed project. This Investment Justification must include:

- A description of the overarching multi-entity project;
- The division of responsibilities among the eligible entities in the group and all participating SLTTs;
- The distribution of funding among the eligible entities in the group, including any subawards; and
- A description of how the project will help implement the Cybersecurity Plan of each entity.

Do multi-entity projects have to be approved by the Cybersecurity Planning Committee of each eligible entity?
Yes. These projects should be included in the application from each participating eligible entity, each approved by the respective Planning Committee and be aligned with each entity's Cybersecurity Plan.

How does the process for multi-entity projects work?
There is no separate funding for multi-entity projects. Instead, they should be considered as group projects where each eligible entity contributes a portion to the overarching effort. Multi-entity projects only include states or territories. There is no local signatory to a multi-entity agreement. However, local funds may be used, with the local's permission as described in the NOFO. With this consent, the multi-entity group can pass through items or services to local governments in lieu of funding. The following provides a general process outline:

- Eligible entities work collaboratively to define the group project and the roles and responsibilities for each eligible entity, including local governments.
- Each eligible entity must have a Cybersecurity Plan that has been approved by DHS.
- The project must improve or sustain capabilities identified in the respective Cybersecurity Plans for each eligible entity.
- The Cybersecurity Planning Committee of each participating eligible entity must approve their portion of the group project.

What must be submitted for multi-entity projects?

Each eligible entity will be required to submit the following as part of the application package:

- A description of the overarching multi-entity project;
- The other participating eligible entities and all participating SLTT entities;
- The division of responsibilities amongst the multi-entity group;
- The distribution of funding from the grant among the eligible entities that comprise the multi-entity group, to include any subawards made to local entities; and
- How the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

CYBERSECURITY BEST PRACTICES

Are SLTT entities required to adopt a specific cybersecurity framework?
No. SLTT entities are not required to adopt a specific framework but are strongly encouraged to review existing frameworks.

Are there specific best practices that SLTT entities will have to adopt?
Yes. Cybersecurity Plans must address how the best practices listed below and the 16 required elements will be implemented across SLTT entities. Adoption is not required immediately, nor by all SLTT entities. Instead, the Cybersecurity Plan should detail the implementation approach over time and how the following will be consistent with the program goal and objectives. In addition to the 16 required elements, the Cybersecurity Plan must discuss the below seven best practices:

- Multi-factor authentication;
- Enhanced logging;
- Data encryption for data at rest and in transit;
- End use of unsupported/end of life software and hardware that are accessible from the Internet;
- Prohibit use of known/fixed/default passwords and credentials;
- The ability to reconstitute systems (backups); and
- Migration to the .gov internet domain.

ALLOWABLE/ELIGIBLE EXPENSES

What can the grant funds be used for?
Eligible entities can use grant funds for:

- Developing the Cybersecurity Plan;
- Implementing or revising the Cybersecurity Plan;
- Paying expenses directly relating to the administration of the grant, which cannot exceed 5% of the amount of the grant award;
- Assisting with allowed activities that address imminent cybersecurity threats confirmed by DHS; and

- Other appropriate activities as noted in the funding notice.

Are there any specific things the funds cannot be used for?
Funds cannot be used for:

- Supplanting state or local funds;
- Recipient cost-sharing contributions;
- Payment of a ransom from cyberattacks;
- Recreational or social purposes, or for any purpose that does not address cybersecurity risks or cybersecurity threats on SLTT information systems;
- Lobbying or intervention in federal regulatory or adjudicatory proceedings;
- Suing the federal government or any other government entity;
- Acquiring land or constructing, remodeling or altering buildings or other physical facilities; or
- Cybersecurity Insurance; or
- Any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity.

Can personnel be hired with grant funds?
Yes, if aligned to the Cybersecurity Plan. Applicants must address how these functions will be sustained when the funds are no longer available in their application.

What equipment or software should be purchased?
Applicants should determine what equipment is most appropriate for their needs based on their Cybersecurity Plan to mitigate cybersecurity risks or gaps.

Is equipment installation considered construction (e.g., installation of fiber optics in a wall or ground)?
Certain equipment installations are not considered to be construction projects, but this will depend on the specific details of each project. If applicable, an Environmental Planning and Historic Preservation review will be required. Most equipment installations (e.g., generators) will be considered to be "construction" and therefore will not be permitted. Please see Section F.3(c) of the NOFO for further information.

ADDITIONAL INFORMATION

Where Can I go For More Information?
For more information please visit www.cisa.gov/CyberGrants.