Fiscal Year 2023 State and Local Cybersecurity Grant Program Frequently Asked Questions

Release Date: ago 7, 2023

Background

In the Infrastructure Investment and Jobs Act, 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, federally recognized tribes are the only eligible entities and do not apply for funding through SAAs.

This Frequently Asked Questions (FAQs) document addresses common questions about the SLCGP. Additional information on the TCGP is forthcoming.

Program Overview

What is the purpose of the State and Local Cybersecurity Grant Program (SLCGP)?

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

Is the SLCGP related to the Homeland Security Grant Program (HSGP)?

No. The SLCGP and the HSGP are completely different DHS programs with separate requirements and criteria. The SAAs for SLCGP and HSGP funds may also be different.

How much funding is available?

For FY 2023, Congress appropriated $400 million. This includes $374.9 million for SLCGP, $12 million for TCGP, $20 million for the Department of Homeland Security to administer the grant, and $1 million for the DHS Inspector General to evaluate the grant program. Congress also appropriated $300 million for FY 2024 and $100 million for FY 2025.

What are the changes in funding levels between program years?

The appropriated funding amount has increased from $200 million in FY 2022 to $400 million in FY 2023. Congress also authorized appropriations of $300 million for FY 2024 and $100 million for FY 2025.

How will funds be allocated?

In FY 2023, $374.9 million is available under the SLCGP. Each state and territory 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. While 80% of total state or territory allocations must support local entities, 25% of the total state or territory allocations must support rural entities.

What is allowable for Management and Administration (M&A)?

A maximum of 5% of a state's SLCGP funding may be used solely for M&A purposes. This 5% is within the 20% the state may retain. Subrecipients can also retain 5% of their award for M&A activities. States are not required to use the maximum 5% of funds for M&A purposes.

M&A costs are for activities directly related to the management and administration of the award, which includes financial management, reporting, and program and financial monitoring. Examples are grants management training for M&A staff, equipment, and supplies for M&A staff to administer the grant award, and travel costs for the M&A staff to conduct subrecipient monitoring. Characteristics of M&A expenses are typically direct costs incurred for administering the federal award, identifiable and unique to each federal award, charged based on the activity performed for that federal award, and not duplicative of the same costs included in the approved Indirect Cost Rate Agreement, if applicable.

For more information on M&A funding, please refer to Section D.13(c) of the NOFO.

When will states and territories receive funding?

For FY 2022 applications, states and territories will receive funding when they receive their "Revised Notice of Grant Award" in the Non-Disaster (ND) Grants system. For FY 2023 applications, states and territories will receive funding when they receive their "Notice of Grant Award" in the ND Grants system.

Who is eligible to apply?

The 56 SAAs for states and territories are the only eligible applicants for SLCGP funding. In addition, two or more eligible entities may jointly apply for assistance as a multi-entity group. Under SLCGP, a multi-entity group is two or more SAAs that apply for joint projects. However, each SAA must submit separate applications.

Local governments can participate in the SLCGP as subrecipients to their state. Local governments interested in participating in the SLCGP should contact their SAAs.

To be eligible for FY 2023 SLCGP funding, each eligible entity is required to fulfill the FY 2022 NOFO requirements. Any state that did not apply in FY 2022, must

satisfy the requirements of the FY 2022 NOFO (i.e., CISA-approved Cybersecurity Plan) before FY 2023 funds will be released. Specifically, the submission of a Cybersecurity Plan, Cybersecurity Planning Committee Membership List, and Cybersecurity Planning Committee Charter that aligns with the criteria detailed in the NOFO, unless the applicant already has a CISA-approved Cybersecurity Plan, Committee List, and Charter. All 56 states and territories are eligible to receive funding for FY 2023 SLCGP after fulfilling the FY 2022 requirements.

For more information on FY 2022 requirements that must be met prior to the development of FY 2023 applications, please refer to Appendices A–C of the NOFO.

What is the year-to-year program difference between FY 2022 and FY 2023?

The FY 2023 SLCGP builds on the previous FY 2022 SLCGP to further support the 2020-2024 DHS Strategic Plan and achieve *Goal 3: Secure Cyberspace and Critical Infrastructure*. Thus, FY 2023 SLCGP applicants must have accomplished FY 2022 requirements before addressing FY 2023 SLCGP objectives.

The primary difference between program years is the shifting focus on objectives. FY 2022 focused on Objective 1, while FY 2023 focuses on Objectives 2 and 3. Once requirements for FY 2022 are met, applicants are required to focus on addressing the next program objectives in FY 2023.

For more detailed information on changes, please refer to the FY 2023 SLCGP Key Changes document.

Are entities required to have established a Cybersecurity Planning Committee and Cybersecurity Plan from the FY 2022 requirements to participate in FY 2023?

Yes. To be eligible for FY 2023 SLCGP funding, each entity is required to have established a Cybersecurity Planning Committee that is composed of members as detailed in the Cybersecurity Planning Committee section below. Each eligible entity must also have submitted and received approval of their Cybersecurity Plan and projects.

There are no new requirements for the Cybersecurity Plans and Cybersecurity Planning Committees in FY 2023. CISA considers Cybersecurity Plans as

strategic living documents that states, and territories may update and resubmit, if desired. Entities must consult with CISA regional staff for plan resubmissions.

For more information on FY 2022 requirements that must be met prior to the development of FY 2023 applications, please refer to Appendices A–C of the NOFO.

What was accomplished in FY 2022?

Of the 56 eligible states and territories applying, 54 submitted applications. CISA and FEMA completed all SLCGP award notifications prior to December 31, 2022. Both CISA and FEMA reviewed all submitted packages to ensure requirements were met or extensions granted.

Applicants progressed in establishing their Cybersecurity Planning Committees and submitting Cybersecurity Plans detailing how the applicant will measure implementation and risk reduction, identification, response, and recovery from cyber threats.

What is the role of the State Administrative Agency?

The SLCGP SAA is responsible for managing the grant application submission and award administration process. Working with the applicant's Cybersecurity Planning Committee, the SAA must ensure at least 80% of the federal funds awarded under the SLCGP are passed through to local entities, including at least 25% to rural communities. After receipt of the grant funds, the pass-through requirement must be met within 45 days of the date when the amendment is issued in the ND Grants system releasing the funding hold and FEMA makes the funding available to the SAA for drawdown.

What are the goal and objectives of the program?

The overarching goal of the program is to assist SLT governments in managing and reducing systemic cyber risks. To accomplish this, FEMA and CISA have 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 SLT 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 FY 2022, the program established a strong foundation to build a sustainable cybersecurity program. Initial priorities included the following, all of which are statutory conditions for receiving grant funding:

- 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.

In FY 2023, the focus is to achieve a secure cyberspace and critical infrastructure that assesses and counters the evolving cybersecurity risks. Priorities include the following, all of which are statutory conditions for receiving grant funding:

- Conduct assessments and evaluations to identify gaps that can be mitigated by individual projects throughout the life of the grant program.
- Adopt key Cybersecurity Best Practices and consult Cybersecurity Performance Goals.

For more information on how to meet these conditions, applicants should refer to Appendices A–B of the NOFO.

What is the process for addressing Imminent Cybersecurity Threats?

Through CISA, only DHS has the authority to confirm imminent cybersecurity threats. Additionally, SLT entities do not have the authority to request the

declaration of an imminent cybersecurity threat

DHS notifies SLT entities of imminent cybersecurity threats as appropriate while FEMA issues an Information Bulletin for reprograming SLCGP funds in support of the specific imminent cybersecurity threat. Afterward, SLCGP SAAs must notify the approved Cybersecurity Planning Committee and Chief Information Officer (CIO), Chief Information Security Officer (CISO), or equivalent official (e.g., Chief Cyber Officer, Governor's cabinet official overseeing cybersecurity), which are responsible for reviewing, prioritizing, and approving projects under SLCGP. Impacted SLT entities should be notified consistent with established governance structures and notification processes within the eligible entity.

To use SLCGP grant funding to address imminent cybersecurity threats, the state or territory must have an approved Cybersecurity Plan. If the SLCGP SAA wants to use funds to address imminent cybersecurity threats, requests must be addressed in the Investment Justification (IJ) for Objective 3. There is no minimum amount that the eligible entity must request or reserve through this IJ and if the eligible entity needs to reallocate funding across its approved IJ to address imminent cybersecurity threats, the eligible entity should collaborate with any subrecipient potentially impacted by the reallocation of funds.

Are the grant-funded projects required to be tied to the Threat and Hazard Identification and Risk Assessment (THIRA)/Stakeholder Preparedness Review (SPR) process?

No. Grant-funded projects are required to be tied to the Cybersecurity Plan only. Applicants are encouraged to leverage the THIRA/SPR process, but it is not a requirement.

For more information on the THIRA/SPR process, please refer to Appendix B: Cybersecurity Planning Committee Charter in the NOFO.

Are there services that recipients are required to participate in?

All SLCGP recipients and subrecipients are required to participate in **CISA Cyber Hygiene Service's Vulnerability Scanning** service. Participation is not required for submission and approval of a grant but is a post-award requirement. (Please note, Web Application Scanning (WAS) was an additional FY 2022 requirement

but was removed from FY 2023.)

Additionally, recipients and subrecipients receiving funding assistance are required to participate in the **Nationwide Cybersecurity Review (NCSR)**. Subrecipients receiving non-funding assistances are not *required* to participate in the NCSR but are encouraged to do so. All SLCGP recipients are strongly encouraged to participate in other memberships.

For more information on required services, please refer to Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources in the NOFO.

How often should the Nationwide Cybersecurity Review (NCSR) be completed?

Entities and subrecipients are required to complete the NCSR during the first year of the award/subaward period of performance and annually thereafter. In FY 2023, the open reporting period for the NCSR is October 1, 2023 – February 28, 2024.

What are the recommended services?

It is strongly encouraged that recipients and subrecipients become members of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and/or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). Membership for these two organizations is free.

In addition, CISA offers a range of free cyber resources for managing risk and strengthening cybersecurity that can be found on the Cyber Resource Hub.

When are the FY 2023 SLCGP key dates?

- July XX, 2023: NOFO
- July XX, 2023: Application Start Date
- September XX, 2023, 5 p.m. ET: Applications due to the ND Grants system

How long is the period of performance?

The period of performance for each grant year will be 48 months. Extensions are allowed only on a case-by-case basis.

How will proposed projects be evaluated?

FEMA will evaluate applications for completeness and applicant eligibility. 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:

- Understanding of current cybersecurity posture and areas for improvement;
- Implementation of security protections commensurate with risk;
- Training of organization personnel in cybersecurity;
- Reduction of the risks the project was designed to address; and
- Completion of the proposed projects within the 4-year period of performance.

Additional details on project evaluation criteria are available in Section E of the NOFO.

Are there any examples or templates we can use?

Grants.gov has templates for:

- The Cybersecurity Plan;
- Investment Justification Planning; and
- Project Worksheet.

These templates can be found on the FY 2023 SLCGP page on grants.gov. As plans are considered sensitive documents, CISA and FEMA will not share any states' specific submission. However, SLCGP SAAs should contact their CISA Regional Staff for more guidance.

Local Governments and Rural Areas

How do local governments apply?

Local governments are eligible subrecipients and must work with their state or territory's SAA for information about applying for SLCGP funds.

How are local governments defined?

“Local government” is defined in 6 U.S.C. § 101(13) as

1. 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;
2. *An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
3. A rural community, unincorporated town or village, or other public entity.

How are rural areas defined?

The FY 2023 SLCGP NOFO includes a definition of rural area: per 49 U.S.C. 5302 “rural” is any area with a population of less than 50,000 individuals. To meet the 25% rural pass-through requirement, the eligible subrecipient must be a local government entity within a rural area (a jurisdiction with a population of less than 50,000 individuals).

Can Tribal governments qualify as subrecipients?

Tribal governments may be eligible as subrecipients and can receive SLCGP funding as a local government. Each SAA may determine whether and how much SLCGP funding to pass through to Tribal governments. DHS does not have the authority to mandate that a certain percentage of SLCGP funds are directed to Tribal governments.

Additionally, $12 million in funding will be directly available to tribal entities under the forthcoming Tribal Cybersecurity Grant Program, for which DHS expects to publish the NOFO in 2023.

How can states and territories involve local entities?

States and territories should include local entities in the Cybersecurity Planning Committee. Proper representation from local entities will ensure their

cybersecurity considerations are relayed. Local governments should be made aware of opportunities where states competitively select local projects that align with their Cybersecurity Plan.

What are local governments required to report? How is it different than the state?

Local government subrecipients are required to participate in the closeout reporting by submitting their closeout materials to the SLCGP SAAs within 90 calendar days of the SLCGP SAA's prime award period of performance end date. After submission from subrecipients, SLCGP SAAs should complete all closeout actions for subawards in time for submission to FEMA during the closeout of the prime award.

SLCGP SAAs must submit the Federal Financial Report (FFR) and Performance Progress Report (PPR). Local government subrecipients are expected to provide their SLCGP SAAs with any information if necessary.

How do local governments receive funds?

Local governments can receive funds in the form of subawards. Local entities interested in receiving SLCGP funds should work with their state's or territory's SAA.

Local governments interested in providing strategic input to shape projects should contact their state or territory's Cybersecurity Planning Committee.

Are states able to impose requirements on subrecipients?

States cannot impose overarching requirements for localities to participate in the SLCGP writ large. However, state entities can attach requirements as a condition for individual projects.

What percentage of the funds must be passed through to local entities?

The SLCGP SAA recipient must pass- through at least 80% of the federal funds provided under the grant. With the consent of the recipients, this pass-through

may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. Rural areas must receive 25% of the total federal award must also go to rural areas. This pass-through to rural areas is a part of the overall 80% pass-through.

The local government pass-through requirement, including the rural area pass-through requirement, does not apply to situations, or to entities, as described below:

1. Grant funding awarded solely to support projects integral to the revision of the state or territory Cybersecurity Plan; or

2. The District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, or the United States Virgin Islands.

What are the requirements for the pass-through grant funds?

States must pass-through 80% of federal funds to local governments and cannot impose unreasonable or burdensome requirements as a condition for receipt of grant funds to local governments. The following must be met to pass-through grant funds:

- The SLCGP SAA must make a firm written commitment to passing through grant funds or equivalent non-funding assistance to subrecipients.
- The SLCGP SAA's commitment must be unconditional (i.e., no contingencies for the availability of SAA funds).
- There must be documentary evidence (i.e., award document, terms, and conditions) of the commitment.
- The award terms must be communicated to the subrecipient.

The signatory authority of the eligible entity must have in writing to FEMA that pass-through requirements were met. A letter of intent or similar will not be sufficient to meet the requirements. After funds are distributed, the SLCGP SAA must self-certify that the pass-through requirement was met.

For more information on the pass-through requirements, please refer to Section F.2 of the NOFO.

What percentage of the funds must be passed through to rural entities?

A minimum of 25% of federal funds must pass-through to rural areas. This 25% pass-through to rural entities contributes to the overall 80% pass-through requirement to local governments. The same four criteria and exceptions for pass-through to local governments also apply to the pass-through to rural areas within those local governments.

Because the pass-through to rural entities is part of the overall 80% pass-through requirement to local governments, SLCGP SAAs must obtain the consent of local governments if intending to pass-through non-funding assistance to rural areas in lieu of funding.

When do states need to pass-through funds to local entities?

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 consent documentation 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.

How can the 80% pass-through requirement be met if the state or territory wants to allocate the value of the funding in the form of services/solutions

procured, managed, and/or deployed by the state or territory?

The SLCGP SAA must pass-through at least 80% of the federal funds provided under the grant. With the consent of the local subrecipients, this pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. Rural areas must receive 25% of the total federal award. This pass-through to rural areas is a part of the overall 80% pass-through. All pass-through entities must meet all program and grant administration requirements.

If a state wishes to pass-through only non-funding assistance, it is recommended that they gauge interest in this funding alternative directly from the local governments by consulting with municipal, city, county, rural communities, or other local government councils or associations. States must also include local governments in their Cybersecurity Planning Committees. Non-funding pass-through must be documented in accordance with the Cybersecurity Planning Committee's Charter.

Pass-through must occur within 45 calendar days of receiving funds. 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.

For more information on passing through non-funding assistance, please refer to Section F.2(e) of the NOFO.

What is the process for selecting which local governments and rural areas will get funds and for which projects?

All pass-through entities must meet all program and grant administration requirements. Cybersecurity Planning Committees must work collaboratively across the state to identify and prioritize individual projects that align with the state's Cybersecurity Plan. If passing through items or services in lieu of funding, ultimately, it is up to the state/territory to determine where and how to pass-through funds, with the permission of applicable local governments.

Do states need to receive consent from every locality within their jurisdiction if passing through non-funding assistance?

No. There may be a large number of potential subrecipients, but SAAs do not need to provide funding to every eligible subrecipient as long as the 80% pass-through (with 25% for rural areas) requirement is met. The 80% pass-through requirement applies to local entities as a whole.

If the state recipient is passing through non-funding assistance in lieu of financial funding, states will need to receive consent from participating localities. The state does not need to request written consent from every single eligible subrecipient to make this decision.

If the participating local government does not consent to having the state provide non-financial assistance in place of funding, then the SLCGP SAA must pass-through funding to that local government in the form of a subgrant award, provided that entity has an approved project as part of the approved Cybersecurity Plan to utilize the funds.

Please note territories are not required to participate in the pass-through requirement.

For more information on engaging local governments, please refer to Section F.2(e) of the NOFO.

Can the 80% pass-through be in a combination of funding and non-funding assistance?

Yes. As long as the total is equivalent to 80% of recipient's federal funding amount, entities can pass-through a combination of financial funds and non-financial assistance.

Are there exceptions to the 80% pass-through requirement?

The local government and rural area pass-through requirement do not apply to situations, or to entities, as described below:

- Grant funding awarded only to support activities integral to the development or revision of the Cybersecurity Plan of the state; or
- The District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, or the United States Virgin Islands.

In the first exception, the SLCGP SAA must submit a proposed budget and budget narrative in the Project Worksheet, along with a written justification outlining how the proposed costs will be used to develop or revise the Cybersecurity Plan to FEMA. Once the proposed costs and activities are reviewed by FEMA and CISA, the SLCGP SAA will be notified, and the funding will be released.

Is there a template of the consent letter?

No. SLCGP SAAs are responsible for creating their own consent documentation. Local consent must be signed by the Authorized Official (or his/her designee) for the local government entity receiving non-funding assistance in lieu of funding, and the consent must specify the amount and intended use of the funds. The SAA's certification 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.

For more information on the consent letter, please refer to Section F.2(d) of the NOFO.

Cost Share

What is a cost share?

A cost share, or cost match, is applicable to eligible entities and multi-entity projects. Eligible applicants will agree to make available non-federal funds to carry out a SLCGP award in an amount that is not less than 20% of activities under the award. The cost share for the multi-entity projects is 10%. To meet requirements, contributions must be certifiable, reasonable, and allocable under the grant program and in compliance with all applicable federal requirements and regulations. Unless otherwise authorized by law, the non-federal cost share

requirement cannot be matched with other federal funds.

What is the required cost share for individual projects?

For applications made by an individual eligible entity, the FY 2023 non-federal cost share requirement is 20%. For FY 2023, cost share requirements are waived for the insular areas of the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

For more information on Cost Share, please refer to Section C.6 of the NOFO.

What is the cost share for a multi-entity project?

Cost share for multi-entity projects in FY 2023 is 10%.

How does the cost share work?

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 20% of the total project costs (federal award amount plus cost share amount). The cost share applies to each individual project funded by the grant award rather than the cumulative total. Recipients must ensure that each activity's cost share is met.

DHS interprets "activity" as all projects approved as part of the submitted Project Worksheets. The Project Worksheets must include cost share and M&A funding for each project objective, as well as a description of the source of the cost share/match. For post-award documentation of cost share, if funds or services are provided by a third party in-kind (soft match), a dated letter of commitment is required to document the donation.

To calculate cost share for a project, please see the formula and example below:

Formula: Total Project Cost x* Cost Share Percentage of the Project = Cost Share Amount; Total Project Cost x Federal Percentage Share of the Project = Federal Amount for the Project

Example: If the total project cost is $125,000, the cost share percentage of the project is 20% and the federal percentage share of the project is 80%, the cost share amount for the project and federal amount for the project is calculated below:

- $125,000 x* .20 = $25,000 (Cost Share Amount for Project)
- $125,000 x* .80 = $100,000 (Federal Share Amount for Project)

For more information on Cost Share, please refer to Section C.6 of the NOFO.

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. SLCGP SAAs that apply 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 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.
- 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.
- Any other factors the Secretary considers appropriate.

To request a cost-share waiver, the SLCGP SAA should submit a waiver request with their FY 2023 SLCGP application submission in the ND Grants system 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.

For more information on the Cost Share waiver, please refer to Section C.6(f) of the NOFO.

How does the cost share waiver process impact the state or territory overall cost share?

The cost share waiver applies to the entire recipient award amount. If the cost share waiver is approved, FEMA will require SAAs to submit an external amendment in ND Grants revising the budget to exclude the cost share. The cost share can be partially or fully waived.

For FY 2023, cost share requirements are waived for the insular areas of the U.S. territories of American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

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;
- Liaising 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 written consent on behalf of all local entities across the eligible entity for services, capabilities, or activities provided by the eligible entity through this program.

What is the Cybersecurity Planning Committee Charter?

The Cybersecurity Planning Committee is directed by a charter that governs the committee. All members of the Cybersecurity Planning Committee must sign and date the charter. The charter must be submitted at the time of application as an attachment in the ND Grants system. Revisions to the Cybersecurity Planning Committee Charter can be made but must be sent to the entity's assigned FEMA Preparedness Officer.

The Cybersecurity Planning Committee Charter must have:

- A detailed description of the Cybersecurity Planning Committee's composition and an explanation of key governance processes;
- A description of the frequency at which the Cybersecurity Planning Committee will meet;

- An explanation as to how the committee will leverage existing governance bodies;
- A detailed description of how decisions on programmatic priorities funded by SLCGP will be made and how those decisions will be documented and shared with its members and other stakeholders, as appropriate; and
- A description of defined roles and responsibilities for financial decision making and meeting administrative requirements.

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 SLT governments;
- Devise a cohesive planning framework;
- Incorporate CISA and FEMA resources as well as those from other federal and SLT entities, and the private sector; 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 projects?

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.

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.

For more information on multi-entity projects, please refer to Section B.10(c.III) of the NOFO.

Are there additional requirements for multi-entity projects?

Yes. In addition to each eligible entity having their own Cybersecurity Planning Committee and CISA-approved Cybersecurity Plan, multi-entity groups must also have a multi-entity Investment Justification for the proposed project. Each participating state or territory group members' Cybersecurity Plans, the IJs and PWs for the multi-entity project must include:

- A detailed description of the overall project;
- The division of responsibilities among each participating state or territory group member entity;
- The distribution of funding among the participating state or territory group member entities; and
- Overview of how implementation of the multi-entity project will help achieve the goals and objectives in the Cybersecurity Plan of each participating entity.

For more information on multi-entity project requirements, please refer to Section B.10(c.III) of the NOFO.

Do multi-entity projects have to be approved by the Cybersecurity Planning Committee of each eligible entity?

Yes. The multi-entity project submissions must be approved by each of the participating state or territory's Cybersecurity Planning Committees, and each of the multi-entity project submissions must be aligned with each of the participating state or territory's respective Cybersecurity Plan.

For multi-entity groups, each participating state or territory must have a CISA-approved Cybersecurity Plan. The project must improve or sustain capabilities identified in the respective Cybersecurity Plan for each eligible entity. Please note that participants in a multi-entity group submit their own Investment Justification.

Can local entities be included in multi-entity projects?

Yes, but since local entities are subrecipients, their eligible entity (i.e., the state SAA) must be participating in the multi-entity project in some capacity. Local entities should be considered as group projects within their state or territory allocations.

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 where it may be typical for a state or territory to take a lead in a multi-entity project. There is no local signatory to a multi-entity agreement. However, local funds may be used, with the local's consent as described in the NOFO. With this consent, the multi-entity group can pass-through non-funding assistance 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.

Each state and territory within a multi-entity group has its own application, including Cybersecurity Plan and Cybersecurity Planning Committee. All members of the multi-entity must have an approved Cybersecurity Plan to receive funding for the multi-entity 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 SLT 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 there specific best practices that SLT 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 SLT entities. Adoption is not required immediately, nor by all SLT 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.

Are there exceptions to the adoption and usage of Cybersecurity Best Practices?

No. SLT entities must eventually adopt and use all seven Cybersecurity Best Practices as listed above. SLT entities cannot forgo the adoption and usage of one or more Cybersecurity Best Practices. The Cybersecurity Best Practices must be addressed in the Cybersecurity Plan, but immediate adoption by the SLT is not required. The adoption of Cybersecurity Best Practices must be implemented within a reasonable timeline as outlined in the Cybersecurity Plan.

Are SLT entities required to transition to the .gov internet domain?

Educational institution subrecipients using .edu are exempted from transiting to the .gov internet domain due to the nature of the .edu internet domain.

All other subrecipients are required to transition to a .gov internet domain. A .gov internet domain not only provides many security benefits but also signals trust and credibility to public users. Cybersecurity Plans should detail the implementation approach of a .gov internet domain over time. Upon completion of the SLCGP, participating entities will only operate under the .gov internet domain and not use .org, .com, or any other domain.

For more information on migrating to the .gov internet domain, please visit the DotGov Program at get.gov

Cybersecurity Plans

Who is required to submit a Cybersecurity Plan?

States and territories that did not apply in FY 2022 or did not complete a Cybersecurity Plan must submit Cybersecurity Plans for review and approval as part of their grant applications. Cybersecurity Plans must be submitted to DHS for review and approval to receive FY 2023 funding.

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 starting in FY 2024. This means that if you have an approved plan from FY 2022, you do not have to submit a new plan for FY 2023; however, states and territories will have to submit an updated plan for FY 2024 SLCGP.

Can I revise my Cybersecurity Plan?

Yes. After initial Cybersecurity Plans are submitted, entities can submit amendments and updates to their Cybersecurity Plan as needed. CISA considers the Cybersecurity Plans as living strategic documents that can be updated and resubmitted, if desired. Entities must work with CISA regional staff on Cybersecurity Plan resubmissions.

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 SLCGP goals, 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 SLT 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.

For more information on Cybersecurity Plan requirements, please refer to Appendix C: Cybersecurity Plan in the NOFO.

What if I receive notice that my Cybersecurity Plan is not compliant?

Eligible entities are encouraged to send their first draft early so that CISA can engage with states and territories on any updates. CISA Regional Staff will work with entities individually on their draft to help make their non-compliant Cybersecurity Plans meet full compliance. A compliant initial plan is not required, and eligible entities should instead focus on submitting a draft as early as possible.

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 SLT information systems.

The projects should achieve a sustainable improvement solution that will remain after the expiration of the cybersecurity grant program. The ultimate goal of the program as stated in the legislation is to award grants that address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, SLT governments. Since the SLCGP is authorized for four years (2022–2025) with limited funds, Cybersecurity Plans must be sustainable enough to continue capabilities once the SLCGP ends or funds are no longer available.

When will I receive funding after my Cybersecurity Plan is approved?

Releasing funds is a two-step process due to the different roles that CISA and FEMA have within the SLCGP. CISA approves Cybersecurity Plans, projects, and associated funding while FEMA releases funds. After the approval of a Cybersecurity Plan, projects and associated funding, FEMA will review any project budgets and, if approved, process an internal amendment to rescind any funding holds and release the funding. Therefore, there may be a short delay in receiving funds after plans and projects are approved.

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, SLT entities.

Does DHS approve the submitted Cybersecurity Plans?

Yes. Once approved by the Cybersecurity Planning Committee, the CIO, 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 and may be referenced as necessary. The template is located on the CISA.gov website.

Can I see an example of an approved Cybersecurity Plan?

As they are sensitive in nature, DHS/CISA/FEMA will not share states or territories specific Cybersecurity Plan. CISA offers a downloaded Cybersecurity Plan template which can be viewed on the CISA.gov website. In addition, SLCGP SAAs can consult with their CISA Regional Staff for more guidance on Cybersecurity Plans.

Is there a required format for the Cybersecurity Plan?

No. There is no required format for the Cybersecurity Plan but required elements must be identifiable for review purposes. Eligible entities are, however, encouraged to review and utilize the provided Cybersecurity Plan Template which includes additional details, samples, and templates.

For more information on the Cybersecurity Plan, please refer to Appendix C: Cybersecurity Plan in the NOFO.

Is there a timeline that the Cybersecurity Plan must cover?

The plan is strategic in nature and recommended to address a two-to-three-year period.

What is the timeline of the Cybersecurity Plan?

For FY 2022 applications, the timeline of a Cybersecurity Plan included:

1. Eligible entities, Cybersecurity Planning Committees, and the CIO/CISO/Equivalent must approve the Cybersecurity Plan. Before submitting, the eligible entity must certify that the Cybersecurity Plan has been formally approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent.
2. Once the Cybersecurity Plan is completed and approved by the Cybersecurity Planning Committee and CIO/CISO/Equivalent, entities must submit updated Investment Justifications for Objectives 1, 2, and 3 (including Objective 4, if applicable).
3. Eligible entities submit their initial Cybersecurity Plan by September 30, 2023.
4. After the initial Cybersecurity Plan is submitted, CISA will review and work with the eligible entities on their draft to ensure the Cybersecurity Plan is compliant and meets all required elements.
5. Once the initial Cybersecurity Plan is finalized, SLCGP SAA Points of Contact will receive a formal approval letter to inform them that their Cybersecurity Plan is approved and meets the SLCGP statutory requirements.
6. After the initial Cybersecurity Plan approval, the Cybersecurity Plan, Cybersecurity Projects, and associated funding are sent to FEMA for budget review.
7. After approval from FEMA, SLCGP SAAs will receive an amendment with the rescission of any funding hold and release the associated funding amount for the approved projects.

Please note that updates on the Cybersecurity Plan can be made over time through amendments and revisions. Mandatory updates to the Cybersecurity Plan are required in FY 2024.

Allowable/Eligible

What can the grant funds be used for?

Eligible entities can use grant funds for:

- 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 NOFO.

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

Funds cannot be used for:

- Spyware
- 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 SLT 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;
- 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, recipients should contact their FEMA Preparedness Officer to address project-specific questions regarding equipment installation. Most equipment installations (e.g., generators) will be considered “construction” and therefore will not be permitted.

For more information on equipment installations, please refer to Section D.13(a) of the NOFO.

Additional information

Where can I go for more information?

For more information, please visit cisa.gov/state-and-local-cybersecurity-grant-program.

What other resources are available to address programmatic, technical, and financial questions?

- For additional support and guidance, SLTs 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.