

## The Department of Homeland Security (DHS)

### Notice of Funding Opportunity (NOFO)

#### Fiscal Year (FY) 2025 State and Local Cybersecurity Grant Program (SLCGP)

Fraud, waste, abuse, mismanagement, and other criminal or noncriminal misconduct related to this program may be reported to the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1 (800) 323-8603 and TTY 1 (844) 889-4357.

### Contents

1. Basic Information.....	4
A. Agency Name .....	4
B. NOFO Title.....	4
C. Announcement Type .....	4
D. Funding Opportunity Number .....	4
E. Assistance Listing Number .....	4
F. Expected Total Funding .....	4
G. Anticipated Number of Awards .....	4
H. Expected Award Range .....	4
I. Projected Application Start Date .....	4
J. Projected Application End Date .....	4
K. Anticipated Funding Selection Date.....	4
L. Anticipated Award Date .....	4
M. Projected Period of Performance Start Date.....	4
N. Projected Period of Performance End Date.....	4
O. Executive Summary .....	4
P. Agency Contact .....	5
2. Eligibility .....	6
A. Eligible Entities/ Entity Types .....	6
B. Project Type Eligibility .....	7
C. Requirements for Personnel, Partners, and Other Parties .....	7
D. Maximum Number of Applications .....	7
E. Additional Restrictions.....	8
F. References for Eligibility Factors within the NOFO.....	8
G. Cost Sharing Requirement.....	8
H. Cost Share Description, Type and Restrictions.....	9
I. Cost Share Calculation Example.....	10
J. Required information for verifying Cost Share.....	11
3. Program Description .....	11
A. Background, Program Purpose, and Program History .....	11
B. Goal, Objectives, and Priorities.....	13
C. Program Rationale.....	18
D. Federal Assistance Type.....	18
E. Performance Measures and Targets .....	18
F. Program-Specific Unallowable Costs .....	19

G.	General Funding Requirements .....	20
H.	Indirect Costs (Facilities and Administrative Costs).....	21
I.	Management and Administration Costs .....	22
J.	Pre-Award Costs.....	23
K.	Beneficiary Eligibility .....	23
L.	Participant Eligibility .....	23
M.	Authorizing Authority .....	23
N.	Appropriation Authority.....	24
O.	Budget Period.....	24
P.	Prohibition on Covered Equipment or Services.....	24
4.	Application Contents and Format .....	24
A.	Pre-Application, Letter of Intent, and Whitepapers .....	24
B.	Application Content and Format .....	24
C.	Application Components.....	24
D.	Program-Specific Required Documents and Information.....	24
E.	Post-Application Requirements for Successful Applicants.....	26
5.	Submission Requirements and Deadlines .....	27
A.	Address to Request Application Package.....	27
B.	Application Deadline.....	29
C.	Pre-Application Requirements Deadline.....	29
D.	Post-Application Requirements Deadline .....	29
E.	Effects of Missing the Deadline .....	29
6.	Intergovernmental Review.....	29
A.	Requirement Description and State Single Point of Contact .....	29
7.	Application Review Information .....	29
A.	Threshold Criteria.....	29
B.	Application Criteria.....	29
a.	<i>Programmatic Criteria</i> .....	29
b.	<i>Review and Selection Process</i> .....	29
c.	Financial Integrity Criteria .....	30
d.	Supplemental Financial Integrity Criteria and Review .....	31
C.	Reviewers and Reviewer Selection .....	31
D.	Merit Review Process.....	31
E.	Final Selection.....	31
8.	Award Notices .....	31
A.	Notice of Award .....	31
B.	Pass-Through Requirements.....	32
C.	Note Regarding Pre-Award Costs .....	34
D.	Obligation of Funds.....	34
E.	Notification to Unsuccessful Applicants.....	34
9.	Post-Award Requirements and Administration .....	34
A.	Administrative and National Policy Requirements .....	34
B.	DHS Standard Terms and Conditions .....	35
C.	Financial Reporting Requirements.....	35
D.	Programmatic Performance Reporting Requirements.....	35
E.	Closeout Reporting Requirements.....	36

F. Disclosing Information per 2 C.F.R. § 180.335 .....	37
G. Reporting of Matters Related to Recipient Integrity and Performance .....	37
H. Single Audit Report .....	37
I. Monitoring and Oversight .....	38
J. Program Evaluation .....	38
K. Additional Performance Reporting Requirements .....	39
L. Termination of the Federal Award .....	39
M. Best Practice .....	41
N. Payment Information .....	41
O. Immigration Conditions] .....	43
10. Other Information .....	43
A. Period of Performance Extension .....	43
B. Other Information .....	43
11. Appendix A: SLCGP Requirements Matrix .....	49
12. Appendix B: Required, Encouraged, and Optional Services, Memberships, and Resources .....	51
13. Appendix C: Sample Performance Progress Report (PPR) and Sample Cyber Performance Narrative for Progress Reporting .....	53
14. Appendix D: POETE Solution Areas for Investments .....	59

**1. Basic Information**

<b>A. Agency Name</b>	U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
<b>B. NOFO Title</b>	Fiscal Year (FY) 2025 State and Local Cybersecurity Grant Program (SLCGP) Notice of Funding Opportunity (NOFO)
<b>C. Announcement Type</b>	Initial
<b>D. Funding Opportunity Number</b>	DHS-25-GPD-137-00-99
<b>E. Assistance Listing Number</b>	97.137
<b>F. Expected Total Funding</b>	\$91,750,000
<b>G. Anticipated Number of Awards</b>	56 awards
<b>H. Expected Award Range</b>	\$255,679 – \$4,174,163
<b>I. Projected Application Start Date</b>	08/1/2025 4:00 p.m. Eastern Time (ET)
<b>J. Projected Application End Date</b>	08/15/2025 5:00 p.m. Eastern Time (ET)
<b>K. Anticipated Funding Selection Date</b>	08/502025
<b>L. Anticipated Award Date</b>	09/09/2025
<b>M. Projected Period of Performance Start Date</b>	09/01/2025
<b>N. Projected Period of Performance End Date</b>	08/31/2029
<b>O. Executive Summary</b>	Our nation faces unprecedented threats to the homeland from increasingly sophisticated criminal groups and nation-state actors. State, local, and territorial (SLT) entities stand at the forefront of cyber defense. This partnership includes enforcing laws, assisting the federal government in securing borders and cyberspace, and dismantling transnational criminal organizations. Cybersecurity threats, including ransomware intrusions, and widespread software vulnerabilities affecting SLT systems and critical infrastructure are increasingly exploited by malicious actors, operating both domestically and abroad. To strengthen the essential partnership DHS maintains with its SLT partners in executing its mission, DHS is

	<p>committed to supporting SLT efforts to combat cybersecurity threats and mitigate risks that endanger these vital functions.</p> <p>Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of SLT governments is the focus of the SLCGP. Through funding from the Infrastructure Investment and Jobs Act, referred to as the Bipartisan Infrastructure Law (BIL) throughout this document, the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies to that strengthen the security of critical infrastructure and improve the cybersecurity resilience of services SLT governments provide their communities.</p>
<b>P. Agency Contact</b>	<p><b>a. <i>FEMA SLCGP Program Office Contact</i></b> The FEMA SLCGP Program Office can provide general information on all FEMA grant programs and additional guidance surrounding questions on SLCGP administration. Applicants and recipients may contact their FEMA Preparedness Officer, the Cyber Section Chief, or the Cyber Branch Chief for more information by email at <a href="mailto:FEMA-SLCGP@fema.dhs.gov">FEMA-SLCGP@fema.dhs.gov</a>.</p> <p><b>b. <i>CISA Grant Program Office Contact</i></b> The Cybersecurity and Infrastructure Security Agency (CISA) Grant Program Office, including programmatic and regional staff, are available to provide general information regarding the SLCGP and additional guidance surrounding programmatic requirements and performance metrics. Applicants and recipients can contact their CISA grant program staff and regional staff for more information by email at <a href="mailto:SLCGPinfo@mail.cisa.dhs.gov">SLCGPinfo@mail.cisa.dhs.gov</a>.</p> <p><b>c. <i>FEMA Grants News</i></b> This channel provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the federal, state, and local levels. FEMA Grants News Team is reachable at <a href="mailto:fema-grants-news@fema.dhs.gov">fema-grants-news@fema.dhs.gov</a> OR (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET.</p> <p><b>d. <i>FEMA Grant Programs Directorate (GPD) Award Administration Division</i></b> FEMA GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. AAD can be contacted at <a href="mailto:ASK-GMD@fema.dhs.gov">ASK-GMD@fema.dhs.gov</a>.</p> <p><b>e. <i>Civil Rights</i></b> <u>Consistent with Executive Order 14173, <i>Ending Illegal Discrimination &amp; Restoring Merit-Based Opportunity</i></u>, the FEMA Office of Civil Rights is responsible for ensuring compliance with and</p>

	<p>enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA. They are reachable at <a href="mailto:FEMA-CivilRightsOffice@fema.dhs.gov">FEMA-CivilRightsOffice@fema.dhs.gov</a>.</p> <p><b>e. <i>Environmental Planning and Historic Preservation</i></b>  The FEMA Office of Environmental Planning and Historic Preservation (OEHP) provides guidance and information about the EHP review process to FEMA programs and recipients and subrecipients. Send any inquiries regarding compliance for FEMA grant projects under this NOFO to <a href="mailto:FEMA-OEHP-NOFOQuestions@fema.dhs.gov">FEMA-OEHP-NOFOQuestions@fema.dhs.gov</a>.</p> <p><b>f. <i>FEMA Grants Outcomes (GO)</i></b>  For technical assistance with the FEMA GO system, contact the FEMA GO Helpdesk at <a href="mailto:femago@fema.dhs.gov">femago@fema.dhs.gov</a> or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET.</p>
--	--

## **2. Eligibility**

<b>A. Eligible Entities/ Entity Types</b>	<p>Only the following entities or entity types are eligible to apply.</p> <p><b>a. <i>Applicants</i></b>  All 56 states and territories, as listed in the definition for “State” below, are eligible to apply for SLCGP funds. The Governor-designated SLCGP State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS.<sup>1</sup> One or more states or territories may submit a multi-entity project.</p> <p>“State” is defined in Section 2 of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 101(17)) to include the 50 states, District of Columbia, Commonwealth of Puerto Rico, U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.</p> <p><b>b. <i>Subapplicants</i></b>  Subapplicants and subawards are allowed. Subapplicants should not have foreign nationals or noncitizens included. If a subapplicant has foreign nationals, they must be properly vetted and must adhere to all government statutes, policies, and procedures including “staff American, stay in America” and security requirements.</p>
---	---

---

<sup>1</sup> As used in this NOFO, “DHS” includes CISA and FEMA, which are components of the U.S. Department of Homeland Security.

	<p>Eligible subrecipients include local governments and do not include nonprofit and for-profit organizations. Section 2(13) of the Homeland Security Act of 2002 (codified as amended at <a href="#">6 U.S.C. § 101(11)</a>) defines local government.</p> <p><b>Other Subaward Information:</b> Public Educational Institutions A public educational institution (e.g., elementary school, secondary school, or institution of higher education) is generally eligible to receive assistance under SLCGP if it is an agency or instrumentality of a state or local government under state and/or local law. In contrast, a private educational institution would not be eligible to receive SLCGP assistance because it is not an agency or instrumentality of a state or local government. “Assistance” means either funding, non-funding assistance (i.e., items, services, capabilities, or activities), or a combination of both. The eligibility of charter schools depends on the function of the charter school—it will be eligible if, and only if, it is an agency or an instrumentality of the state or local government.</p> <p>The SAA for an SLCGP grant award is responsible for demonstrating the eligibility of each entity receiving assistance, as described in section 2b. above, and should consult with DHS if there is uncertainty regarding eligibility for a particular entity.</p>
<b>B. Project Type Eligibility</b>	<p><b>a. <i>Unallowable Costs for SLCGP Projects</i></b> Unallowable costs are described in Section 3.G, “<a href="#">Program-Specific Unallowable Costs</a>” in this NOFO.</p> <p><b>b. <i>Allowable Costs for SLCGP Projects</i></b> Please see the Appendix D, “<a href="#">Planning, Organization, Equipment, Training, and/or Exercises (POETE) Solution Areas for Investment</a>” for more information on allowable costs related to the POETE Solution Areas.</p> <p>Allowable SLCGP costs, pre-award costs, M&amp;A costs and indirect costs are described in <a href="#">Section 3.H – 3.J</a>.</p>
<b>C. Requirements for Personnel, Partners, and Other Parties</b>	<p>Subapplicants should not have foreign nationals or noncitizens included. If a subapplicant has foreign nationals, they must be properly vetted and must adhere to all government statutes, policies, and procedures including “staff American, stay in America” and security requirements.</p> <p>Subapplicants/subrecipients must submit short bios and resumes. This should include the type of entity, organizational leadership, and board members along with the both the names and addresses of the individuals. Resumes are subject to approval.</p>
<b>D. Maximum Number of Applications</b>	<p>The maximum number of applications that can be submitted is:</p> <ol style="list-style-type: none"> <li>1. A maximum of one application per eligible entity.</li> </ol>

<b>E. Additional Restrictions</b>	Applicants/subapplicants or recipients/subrecipients are required to certify their compliance with federal statutes, DHS directives, policies, and procedures.
<b>F. References for Eligibility Factors within the NOFO</b>	<p>Please see the following references provided below:</p> <ol style="list-style-type: none"> <li>1. “Responsiveness Review Criteria” subsection</li> <li>2. <a href="#">“Financial Integrity Criteria”</a> subsection</li> <li>3. <a href="#">“Supplemental Financial Integrity Criteria and Review”</a> subsection</li> <li>4. FEMA may/will request financial information such as Employer Identification Number (EIN) and bank information as part of the potential award selection. This will apply to everyone prospered, including subrecipients.</li> </ol> <p>All recipients are required to submit the following documentation:</p> <ol style="list-style-type: none"> <li>1. Cybersecurity Plan (resubmission, if required)</li> <li>2. Cybersecurity Planning Committee Membership List and Charter</li> </ol> <p>All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA, with specific requirements depending upon the entity and type of funding received. Additional information on SLCGP requirements are detailed in Appendix A, <a href="#">“SLCGP Requirements Matrix”</a> and Appendix B, <a href="#">“Required, Encouraged, and Optional Services, Memberships, and Resources.”</a></p>
<b>G. Cost Sharing Requirement</b>	<p>Applicants selected for this award must agree to an acceptable cost share agreement. Otherwise, they will not be funded. For FY 2025, in accordance with 48 U.S.C. § 1469a, 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.</p> <p>Project-based Cost Share: Section 2220A of the Homeland Security Act of 2002 requires a state to meet a nonfederal matching requirement for an “activity” carried out under an SLCGP grant award. DHS interprets the term “activity” to be an approved “project” under an SLCGP grant award and administers the nonfederal matching requirement in accordance with 2 C.F.R. § 200.306.</p> <p>Eligible applicants must agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 40% of the total project costs (federal award amount plus cost share amount, rounded to the nearest whole dollar). The cost share for the multi-entity projects is 30% for FY 2025.</p>



<p><b>H. Cost Share</b> <b>Description, Type</b> <b>and Restrictions</b></p>	<p>DHS administers cost-matching requirements in accordance with 2 C.F.R. § 200.306. To meet matching requirements, the recipient contributions must be verifiable, reasonable, allocable, and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations. The non-federal cost share requirement cannot be matched with other federal funds, unless specifically authorized by the legislation governing that other source of federal funding.</p> <p>The cost share applies to each project funded by the grant award rather than just to the cumulative total of all projects. Recipients must ensure that each project's cost share is met. A Project Worksheet (PW) must include cost share for each project as well as Management and Administration (M&amp;A). M&amp;A must be included as a separate row in the PW. Also, the PW must include a description of the source of the cost share. Note for post-award documentation of cost share, if funds or services are to be provided by a third-party for in-kind match, a dated letter of commitment is required to document the donation. The recipient contribution can be cash (hard match) or third-party in-kind (soft match).</p> <p><b>Types of Cost Share/Match</b></p> <ol style="list-style-type: none"> <li>1. Hard Match (Cash) Cash or hard matching includes cash spent for project-related costs. The allowable cash match must include costs that are necessary, reasonable, and allowable under the SLCGP. State or local general fund monies is an example of hard match.</li> <li>2. Soft Match (In-kind) Soft match refers to contributions of the reasonable value of property or services in lieu of cash which benefit a federally assisted project or program. This type of match may only be used if not restricted or prohibited by program statute, regulation, or guidance and must be supported with source documentation. Only property or services that comply with program guidance and/or program regulations, are allowable. In other words, a recipient cannot use a source for the soft match that is completely unrelated to the SLCGP's goals, objectives, and allowable costs identified in the NOFO, etc. The same contribution cannot be used if it is already used as match for another grant program or paid from other grant funds. Below are some examples of allowable soft match: <ol style="list-style-type: none"> <li>a. <b>Example 1:</b> A hotel offers a room or space to conduct a cybersecurity training event or tabletop exercise. The hotel manager should provide the SAA with written documentation of the room rental (dollar value), date/time of the donation,</li> </ol> </li> </ol>
--	--

	<p>signed by the hotel manager. This should align with the date/time of the training or exercise event. And, per 2 C.F.R. 200.306, “The value of donated space must not exceed the fair rental value of comparable space as established by an independent appraisal of comparable space and facilities in a privately-owned building in the same locality.”</p> <p>b. <b>Example 2:</b> Contributions of salary, travel, equipment, supplies, and other budget areas that are from third-party sources (in compliance with 2 C.F.R. 200.306) and include voluntary contributions such as emergency personnel, lawyers, etc., who donate their time to a federal grant program. The normal per hour rate for these professionals (acting in their professional capacity) can be used to meet the matching requirement. The value of the services provided is taken into consideration when determining the value of the contribution and not who is providing the service. For example, if a lawyer is volunteering his/her services to assist the Cybersecurity Planning Committee with preparing and filing legal paperwork for their Charter, the lawyer’s normal hourly rate is allowable. However, if the lawyer is volunteering his/her time and services to conduct cybersecurity needs assessments as part of the state’s cybersecurity plan implementation, the lawyer’s hourly rate would <u>not</u> be applicable. Instead, the hourly rate for an information technology specialist would be more reasonable and applicable.</p>
<p><b>I. Cost Share Calculation Example</b></p>	<p><b><i>Calculating Cost Share for the Application on the Project Worksheet</i></b></p> <p><b>Formula:</b> Federal Award Amount / Federal Share Percentage = Total Project Cost</p> <p>Cost Share Percentage = Cost Share Amount (rounded up to the nearest whole dollar)</p> <p><b>Example:</b> If the federal award is \$1,000,000 with a 60% federal share percentage and a 40% cost share percentage, the cost share amount is calculated below:</p> <ul style="list-style-type: none"> <li>• \$1,000,000 (Federal Award Amount) / .60 = \$1,666,667 (Total Project Cost)</li> <li>• \$1,666,667 x .40 = \$666,667 (Cost Share Amount)</li> </ul> <p><b><i>Calculating Cost Share for Projects on the Project Worksheet</i></b></p> <p>Cost share must be provided on a project basis. To calculate cost share for a project, please see the following formula and example:</p>

	<p><b>Formula:</b> 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</p> <p><b>Example:</b> If the total project cost is \$125,000, the cost share percentage of the project is 40% and the federal percentage share of the project is 60%, the cost share amount for the project and federal amount for the project is calculated below:</p> <ul style="list-style-type: none"> <li>• \$125,000 x .40 = \$50,000 (Cost Share Amount for Project)</li> <li>• \$125,000 x .60 = \$75,000 (Federal Share Amount for Project)</li> </ul>
<b>J. Required information for verifying Cost Share</b>	<p>Applicants are not required to submit documents to verify cost share (or match) in the pre-award phase. However, applicants are required to include the source of the cost share on the Project Worksheet as part of their application submission.</p> <p><b>Cost Share Documentation for soft match:</b> The source documentation for the cost share should be:</p> <ol style="list-style-type: none"> <li>1. Valued at the time of the donation—value must not exceed the fair market value of the equipment of the same age and condition at the time of donation.</li> <li>2. Signed and dated by the donating company, person, etc.</li> <li>3. For third-party in-kind contributions, the fair market value of goods and services must be documented and, to the extent feasible, supported by the same methods used internally by the non-federal entity.</li> </ol> <p>Please see the “<a href="#">Application Format and Contents</a>” section for details.</p>

### **3. Program Description**

#### **A. Background, Program Purpose, and Program History**

Our nation faces unprecedented threats to the homeland from increasingly sophisticated criminal groups and nation-state actors. SLT entities stand at the forefront of cyber defense, enforcing laws, assisting the federal government in securing borders, cyberspace, and dismantling transnational criminal organizations. Cybersecurity threats, including ransomware intrusions, and widespread software vulnerabilities affecting SLT systems and critical infrastructure, are increasingly exploited by malicious actors, operating both domestically and abroad. To strengthen the essential partnership DHS maintains with its SLT partners in executing its mission, DHS is committed to supporting SLT efforts to combat cybersecurity threats and mitigate risks that endanger these vital functions.

Considering the risk and potential consequences of cyber incidents, the focus of the SLCGP is strengthening the cybersecurity practices and resilience of SLT governments. Through funding from the Infrastructure Investment and Jobs Act, referred to as the Bipartisan Infrastructure Law (BIL) throughout this document, the SLCGP enables DHS to make targeted cybersecurity

investments in SLT government agencies to strengthen the security of critical infrastructure and improve the resilience of services SLT governments provide their communities.

### **FY 2025 SLCGP Allocations**

For FY 2025, DHS will award funds to states and territories based on baseline minimums and population as required by section 2200A(l) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 665g(l)), described below.

Each state and territory will receive a baseline allocation using thresholds established in section 2200A(l) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 665g(l)). All 50 states, the District of Columbia, and the Commonwealth of Puerto Rico will receive a minimum of \$1,000,000 each, equaling 1% of total funds made available for the SLCGP in FY 2025. Each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) will receive a minimum of \$250,000 equaling 0.25% of the total funds made available for the SLCGP in FY 2025. Additionally, \$19,375,000, 50% of the remaining amount, will be apportioned based on the ratio that the population of each state or territory bears to the population of all states and territories. The remaining \$19,375,000 equaling the other 50% of the remaining amount, will be apportioned based on the ratio that the population of each state that resides in rural areas bears to the population of all states that resides in rural areas.

**If a state or territory does not apply, its initial allocation will be redistributed to the other states and territories per the statutory formula. Final allocation amounts will be determined after the Application Deadline date.** Applicants will be notified of the final allocation amounts and required cost share after the Application Deadline.

State/Territory	FY 2025 SLCGP Initial Allocation	State/Territory	FY 2025 SLCGP Initial Allocation
Alabama	\$1,906,331	Nevada	\$1,238,972
Alaska	\$1,114,897	New Hampshire	\$1,248,490
Arizona	\$1,657,942	New Jersey	\$1,703,280
Arkansas	\$1,563,226	New Mexico	\$1,275,083
California	\$3,872,566	New York	\$2,849,577
Colorado	\$1,572,832	North Carolina	\$2,638,773
Connecticut	\$1,351,842	North Dakota	\$1,132,581
Delaware	\$1,108,818	Ohio	\$2,480,716
District of Columbia	\$1,039,593	Oklahoma	\$1,639,860
Florida	\$2,864,442	Oregon	\$1,478,977
Georgia	\$2,448,068	Pennsylvania	\$2,612,850
Hawaii	\$1,137,967	Rhode Island	\$1,091,720
Idaho	\$1,280,792	South Carolina	\$1,793,404
Illinois	\$2,195,011	South Dakota	\$1,162,200
Indiana	\$1,958,035	Tennessee	\$2,090,099
Iowa	\$1,523,385	Texas	\$4,174,163
Kansas	\$1,403,652	Utah	\$1,298,406
Kentucky	\$1,795,927	Vermont	\$1,157,136

Louisiana	\$1,637,992	Virginia	\$2,109,454
Maine	\$1,323,383	Washington	\$1,821,882
Maryland	\$1,612,166	West Virginia	\$1,382,386
Massachusetts	\$1,581,107	Wisconsin	\$1,898,770
Michigan	\$2,346,859	Wyoming	\$1,096,930
Minnesota	\$1,791,614	Puerto Rico	\$1,251,691
Mississippi	\$1,625,367	U.S. Virgin Islands	\$256,150
Missouri	\$1,898,390	American Samoa	\$256,291
Montana	\$1,212,152	Guam	\$263,579
Nebraska	\$1,266,545	Northern Mariana Islands	\$255,679
<b>Total</b>		<b>\$91,750,000</b>	

## **B. Goal, Objectives, and Priorities**

### **a. Goal**

The goal of the SLCGP is to assist SLT governments with managing and reducing systemic cyber risk. This goal can be achieved over the course of the four years of SLCGP funding as applicants focus their Cybersecurity Plans, priorities, projects, and implementation toward addressing SLCGP objectives.

### **b. Objectives**

Applicants are required to submit applications that address at least one of the following program objectives in their applications:

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

Applicants should refer to the CISA website at [www.cisa.gov/cybergrants/slcgp](https://www.cisa.gov/cybergrants/slcgp) for more information on SLCGP priorities, cybersecurity plans, committees and charters, as well as the required program goals, objectives, sub-objectives and desired outcomes for the FY 2025 SLCGP application.

### **c. Priorities**

#### **Cybersecurity Plans, Committees, and Charter**

The Homeland Security Act of 2002, as amended by the BIL, requires SLCGP grant recipients to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the plan, and identify projects to implement using SLCGP funding.

With the FY 2022 SLCGP, recipients were directed to accomplish the following, and for any eligible entities who have not yet applied for SLCGP funding, the following also applies in FY 2025:

- Establish a Cybersecurity Planning Committee; Members must include:
  - The eligible entity;
  - The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or equivalent official (e.g., Chief Cyber Officer, Governor’s cabinet official overseeing cybersecurity) of the eligible entity;
  - Representatives from counties, cities, and towns within the jurisdiction of the eligible entity;
  - Institutions of public education and health within the jurisdiction of the eligible entity; and
  - As appropriate, representatives of rural, suburban, and high-population jurisdictions.
 For updates to the state’s Cybersecurity Committees and Charters, CISA encourages members to include:
  - Representatives from local law enforcement or emergency services; and
  - Representatives from other critical infrastructure sectors.
- Develop a state-wide Cybersecurity Plan, unless the recipient already has a state-wide Cybersecurity Plan; and
- Use SLCGP funds to implement or revise a state-wide Cybersecurity Plan.

Applicants should refer to the CISA website at [www.cisa.gov/cybergrants/slcgp](https://www.cisa.gov/cybergrants/slcgp) for further information about the Cybersecurity Plans, Committees, and Charters.

### **Cybersecurity Activities**

The SAA must consult with its Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) (or an equivalent official of the eligible entity) regarding the plans for allocating SLCGP funds. To support the FY 2025 SLCGP requirements, Cybersecurity Plans must include the following activities:

- Conducting assessment and evaluations as the basis for individual projects throughout the life of the program; and
- Prioritizing, where applicable, key cybersecurity best practices and consulting the [Cybersecurity Performance Goals \(CPGs\)](#).
  - The CPGs are a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.
  - These goals are applicable across all critical infrastructure sectors and are informed by the most common and impactful threats and adversary tactics, techniques, and procedures observed by CISA and its government and industry partners, making them a common set of protections that all critical infrastructure entities—from large to small—should implement.
  - The CPGs do not reflect an all-encompassing cybersecurity program. Rather, they are a minimum set of practices that organizations should implement toward ensuring a strong cybersecurity posture.
  - The Cross-Sector CPGs are regularly updated, with a targeted revision cycle of at least every 6 to 12 months.

### Key Cybersecurity Best Practices for Individual Projects

To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, SLT governments must take decisive steps to modernize their approach to cybersecurity. As SLT governments increase their cybersecurity maturity, CISA recommends they move toward implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing. To assist in the revision of SLT cyber planning efforts, the following Cybersecurity Best Practices are provided. As appropriate, the strategic elements listed in the table below should be included in FY 2025 individual projects:

Cybersecurity Best Practices for Individual Projects	
Implement multi-factor authentication.	
Implement 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.	
Ensure the ability to reconstitute systems (backups).	
Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.	
Migration to the .gov internet domain.	

### Cybersecurity Investments and Projects

Given the Cybersecurity Plan is a strategic document, it should not identify specific vulnerabilities but instead capture the broad level of capability across the jurisdiction. The Cybersecurity Plan must also show how the implementation of the individual projects and activities over time will help achieve the goals and objectives of the plan. The summary of projects using FY 2025 SLCGP funds associated with each required and discretionary element provides a helpful snapshot of state and territory-wide capabilities and capacity that will be achieved as a result of this funding. Details for each project using SLCGP funds must be included in the Investment Justifications (IJs) and the corresponding Project Worksheet (PW).

Each IJ must provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces, which have influenced the development of the IJ. The IJ must include a summary of the current capabilities within the applicant jurisdiction to address these threats and risks. The IJ should also include a description of how the proposed project addresses gaps identified in or sustainment of the approved Cybersecurity Plan, and how the project aligns to the cybersecurity elements in this NOFO. Finally, the IJ should include implementation planning data to assist in project management.

The PW will be used to identify the budget details and budget narrative portion of the application. Eligible applicants should submit only one PW as part of the overall application and must include information for each IJ submitted as part of the application for funding. More information on the IJ Form, PW, and instructions can be found in [Section 4. D](#) in this funding notice.

## **Multi-Entity Projects**

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

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.

### **a. *Timing***

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

### **b. *Nature of a Multi-Entity Project***

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

### **c. *Cooperating Purchasing***

To foster greater economy and efficiency, two states may conduct a joint procurement or pursue some other type of cooperative purchasing arrangement to procure equipment, supplies, or services. Such a collaborative procurement action does not mean that the states are pursuing a multi-entity project. Rather, it is the substance of the underlying scope of work that makes a project a multi-entity project and not the manner in which a state is procuring services in accomplishing a project's scope of work.

The following examples help illustrate the considerations above.

**Example 1:** State X and Y seek to jointly conduct cybersecurity training of their state personnel. Rather than each state conducting its own \$250K worth of training for their respective employees, they want to work together to have joint training sessions so that all trainees get \$500K worth of training. There will be ten training sessions for all state X and Y employees and



each state will be responsible for organizing and executing five sessions. The states, furthermore, jointly conduct a procurement to obtain a contractor that will provide services to help the state carry out all ten sessions. This would be a multi-entity project because both states have to work together to carry out the scope of work, each state is implementing the cybersecurity plan of each other's by training the other state's employees, and there is a shared project objective.

**Example 2:** State X and Y seek to conduct cybersecurity training for their own staffs. To obtain greater cost-savings, the states jointly procure a contractor to conduct their cybersecurity training. Following the procurement, each state runs their own training program and uses the same contractor in doing so. This is not a multi-entity project. This is because each state could accomplish their respective project without working together with the other state to carry out the scope of work, one state is not implementing the cybersecurity plan of the other state by carrying out activities to reduce cybersecurity threats and cybersecurity risks to the other state's information systems, and there is no shared project objective.

### **Multi-Entity Project Requirements and Process Overview**

The following must be included in each of the participating state or territory group members' Cybersecurity Plans, IJs, and PWs for the multi-entity project:

- 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.

### **Multi-Entity Project Benefits**

A multi-entity project is funded from each participating state or territory group members' SLCGP award in accordance with their agreed-upon contribution amounts. Since the multi-entity group may be comprised of state and territory governments, each can benefit from information sharing and awareness opportunities. Multi-entity projects may permit smaller state and territory entities to combine resources with larger state and territory entities to reap the benefits associated with larger acquisitions. At the same time, all parties to a multi-entity project may realize cost savings due to volume purchases. Lastly, the non-federal cost share in FY 2025 SLCGP for the projects in a multi-entity project is 30%.

### **Imminent Cybersecurity Threat**

The SLCGP is primarily a security preparedness program focused on reducing cyber risks by helping SLT entities address cybersecurity vulnerabilities and build cybersecurity capabilities. Over time, the program activities and investments reduce the potential impact of cybersecurity threats and incidents. Section 2220A(d)(4) of the Homeland Security Act of 2002 (codified as amended at 6 U.S.C. § 665g(d)(4)) provides that "An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section" may also use the grant to "assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the [CISA] Director, to the information systems owned or

operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity.”

The following provides an overview of the imminent cybersecurity threat process for the FY 2025 grant cycle. Details on CISA’s criteria and process for confirming an imminent cybersecurity threat are not included here. The following also does not supersede or replace existing threat notification procedures or existing methods to collaborate on operational cybersecurity matters.

### **Process Overview**

- Any eligible entity using SLCGP funds to address an imminent cybersecurity threat, as confirmed by the Secretary, acting through the CISA Director, must have a Cybersecurity Plan approved by CISA.
- DHS, through CISA, will determine if an incident constitutes as an imminent cybersecurity threat.
- Upon confirmation, DHS will notify the SLCGP SAA, and the SAA must notify the state or territory Cybersecurity Planning Committee and CIO/CISO/equivalent.
- DHS will notify impacted SLT entities, as appropriate, of permissible activities to address imminent cybersecurity threats to the information systems owned or operated by, or on behalf of, SLT entities.
- DHS will issue an Information Bulletin detailing the impacted entities and procedures for reprogramming SLCGP funds in support of the specific imminent cybersecurity threat. The scope of the Information Bulletin will be dependent on the nature of the imminent cybersecurity threat.

### **C. Program Rationale**

SLCGP is authorized under the Homeland Security Act of 2002, Pub. L. No. 107-296, § 2220A (codified as amended at 6 U.S.C. § 665g).

### **D. Federal Assistance Type**

Grant

### **E. Performance Measures and Targets**

DHS will communicate with all SLCGP SAA recipients on the information collection process related to performance measures data. To gauge overall program performance, recipients are required to report on the performance measures that are relevant to their plan implementation.

No.	Performance Measures
1	Percentage of entities conducting annual tabletop and full-scale exercises to test Cybersecurity Plans (40% target range).
2	Amount of grant funds budgeted for cybersecurity exercises (10% target range).
3	Percentage of grant funds expended on exercise plans for entities (10% target range).
4	Percentage of entities conducting annual cyber risk assessments conducted to identify cyber risk management gaps and areas for improvement (80% target range).
5	Percentage of entities performing phishing training (70% target range).
6	Percentage of entities conducting awareness campaigns (90% target range).

No.	Performance Measures
7	Percentage of entities providing role-based cybersecurity awareness training (90% target range).
8	Percentage of entities with capabilities to analyze network traffic and activities related to potential threats (60% target range).
9	Percentage of entities implementing multi-factor authentication (MFA) for all remote access and privileged accounts (70% target range).
10	Percentage of entities with programs to anticipate and discontinue end-of-life software and hardware (90% target range).
11	Percentage of entities prohibiting the use of known/fixed/default passwords and credentials (90% target range).
12	Percentage of entities operating under the “.gov” internet domain (70% target range).
13	Percentage of entities that reported CISA-identified Cybersecurity Gaps (50% target range).
14	Percentage of entities with Endpoint Detection Response systems that were funded for implementation (90% target range).
15	Number of capabilities ratings improved (50% target range).
16	Percentage of state/territory-created performance metrics that were met (50% target range).
17	Percentage of entities participating in CISA services (50% target range).
18	Percentage of entities that have implemented data encryption projects (50% target range).
19	Percentage of entities that have implemented enhanced logging projects (60% target range).
20	Percentage of entities that have implemented system reconstitution projects (60% target range).

#### **F. Program-Specific Unallowable Costs**

For FY 2025 SLCGP, grant funds may not be used for the following:

- a. Spyware;
- b. Construction;
- c. Renovation;
- d. To pay a ransom;
- e. For recreational or social purposes;
- f. To pay for cybersecurity insurance premiums;
- g. Costs associated with the Center for Internet Security (e.g., Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis (EI-ISAC)), including but not limited to membership fees and services;
- h. For 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 that receives the grant or a local government within the jurisdiction of the eligible entity;
- i. To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT entity has previously used SLT funds to support the same or similar uses;
- j. For any recipient or subrecipient cost-sharing contribution; and
- k. To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building modifications; see [Minor Modifications Information Bulletin No. 523](#)); Unallowed “alterations” include

permanent modifications that substantially affect the building's structure, layout, or systems, affect critical aspects of a building's safety (such as structural integrity, fire safety systems), or other modifications that materially increase the value or useful life of the building.

- Examples of the types of alterations that are unallowable with SLCGP funding, or the non-federal cost share, are listed below:
  - Updating an electrical system to a building which involves work to enhance or modernize the electrical infrastructure, such as replacing electrical panels, upgrading old or unsafe wiring, and replacing circuit breakers. This type of work is likely a modification that substantially affects the building's systems and thus would comprise an alteration.
  - Installing new walls or reconfiguring existing ones.
  - Affixing equipment in such a way that it becomes a permanent part of a building (as this would result in the equipment no longer being personal property).

### **G. General Funding Requirements**

Costs charged to federal awards (including federal and non-federal cost share funds) must comply with applicable statutes, rules and regulations, policies, this NOFO, and the terms and conditions of the federal award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered within the budget period. [2 C.F.R. § 200.403\(h\)](#).

Recipients may not use federal funds or any cost share funds for the following activities:

1. Matching or cost sharing requirements for other federal grants and cooperative agreements (see [2 C.F.R. § 200.306](#)).
2. Lobbying or other prohibited activities under [18 U.S.C. § 1913](#) or [2 C.F.R. § 200.450](#).
3. Prosecuting claims against the federal government or any other government entity (see [2 C.F.R. § 200.435](#)).

Recipients and subrecipients may use SLCGP funding to perform minor modifications that **do not** substantially affect a building's structure, layout, or systems, affect critical aspects of a building's safety, or otherwise materially increase the value or useful life of the building. The prohibition would also apply to the nonfederal cost-sharing requirement borne by the recipient and/or subrecipient. As a reminder, all projects and associated SLCGP costs must support the approved Cybersecurity Plan and be approved in advance by CISA.

Examples of the types of minor modifications that could be **allowable** with SLCGP funding, and the non-federal cost share are listed below:

- Fastening equipment to walls where it does not become a permanent fixture (such as hanging a server rack with servers on a wall).
- Replacing an outdated existing electrical or internet outlet into which the equipment will connect.
  - For example, replacing an electrical outlet would involve turning off power, unscrewing a cover plate and outlet itself, pulling the outlet from the electrical box, disconnecting wires from the old outlet, connecting the wires to the new outlet, placing the new outlet in the electrical box, securing it with screws, reattaching the

cover plate, and turning the power back on. This work very clearly does not involve a substantial change to the building and does not comprise an alteration.

- Installing new cabling.
- Replacing existing cabling.
- Moving cabling.
- Installing and connecting information system equipment to the building's network and power supply and internet.
- Making a hole in the wall to attach the equipment to the building's network, power, or internet.

Minor modifications may be permitted under the SLCGP subject to Environmental and Historic Preservation (EHP) review. Therefore, recipients (and subrecipients through the SAA) are required to submit their projects for minor building modifications to the FEMA GPD EHP Branch. The protocol for EHP submittal is as follows:

1. The SAA submits the completed EHP Screening form and photos to the FEMA GPD EHP inbox ([GPDEHPinfo@fema.dhs.gov](mailto:GPDEHPinfo@fema.dhs.gov)) with a cc to their SLCGP Preparedness Officer (PO) and [FEMA-SLCGP@fema.dhs.gov](mailto:FEMA-SLCGP@fema.dhs.gov). Additional EHP information can be found at: [Environmental Planning and Historic Preservation | FEMA.gov](#).
2. During the EHP review process, if additional information is needed or is sent to the Regional EHP Office (this is done if the project requires FEMA to consult another agency regarding the project), the SAA and PO are notified via email.
3. Once the EHP review process has been completed, the PO will be notified via email with the EHP Review Completion Letter. The PO will then notify the SAA the EHP review is completed and forwards the EHP Review Completion Letter to the SAA. This letter is important because it contains Standard Conditions and any Special Conditions related to the EHP review and communicates it to the SAA.

Applicants should refer to Appendix D, “[POETE Solution Areas for Investments](#)” for more information on allowable costs related to the POETE Solution Areas.

## **H. Indirect Costs (Facilities and Administrative Costs)**

Indirect costs are allowed for recipients and subrecipients.

Indirect costs (IDC) are costs incurred for a common or joint purpose benefiting more than one cost objective and not readily assignable to specific cost objectives without disproportionate effort. Applicants with a current negotiated IDC rate agreement who desire to charge indirect costs to a federal award must provide a copy of their IDC rate agreement with their applications. Not all applicants are required to have a current negotiated IDC rate agreement. Applicants that are not required to have a negotiated IDC rate agreement, but are required to develop an IDC rate proposal, must provide a copy of their proposal with their applications. Applicants without a current negotiated IDC rate agreement (including a provisional rate) and wish to charge the de minimis rate must contact FEMA for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must contact FEMA for further instructions. As it relates to the IDC for subrecipients, a recipient must follow the requirements of [2 C.F.R. §§ 200.332](#) and [200.414](#) in approving the IDC rate for subawards.

### **Unrecovered Indirect Costs**

With prior approval by DHS, recipients may use unrecovered indirect costs for the cost share for FY 2022–2025 SLCGP awards. All requests to use unrecovered indirect costs for cost share must be submitted to your FEMA SLCGP Preparedness Officer for consideration and approval. Please see [Information Bulletin No. 508](#) for additional details. Recipients will be notified in writing if approval is granted.

### **Establishing Indirect Cost Rates**

The processes for establishing the indirect cost rate vary based on the type of entity and the amount of funding they receive:

1. If the entity is a non-governmental entity, and is a subrecipient, indirect cost rate procedures are outlined in 2 C.F.R. § 200.332(b)(4). These types of entities may either use the de minimis rate or negotiate a rate with the pass-through entity.
2. If the subrecipient is a governmental department or agency, indirect cost rate procedures are established in 2 C.F.R. Part 200, Appendix VII. Per Paragraph D.1.a. of Appendix VII, all departments or agencies of the governmental unit desiring to claim indirect costs under Federal awards must prepare an indirect cost rate proposal and related documentation to support those costs.
3. If the governmental department or agency receives more than \$35 million in grant funding in a fiscal year, the proposal must be approved by the cognizant agency. 2 C.F.R. Part 200, Appendix VII, Paragraph D.1.b.
4. If a governmental department or agency receives \$35 million or less in grant funding in a fiscal year, they must develop an indirect cost rate proposal, but that indirect cost rate proposal does not need to be approved by the cognizant agency. 2 C.F.R. Part 200, Appendix VII, Paragraph D.1.c.
5. If a state, local governmental, or tribal entity wants to use the de minimis rate (instead of developing an indirect cost rate proposal), they can request a case-by-case exception from FEMA (per 2 C.F.R. § 200.102(b)).

### **I. Management and Administration Costs**

M&A costs are allowed.

A maximum of up to 5% of SLCGP federal funds awarded may be retained by the SAA, and any funds retained are to be used solely for M&A purposes associated with the SLCGP award.

Subrecipients (state agencies or local units of government) may also retain a maximum of up to 5% of the federal funding passed through by the state solely for M&A purposes associated with the SLCGP award. While the eligible entity may retain up to 5% of this total for M&A, the state must still ensure that all subrecipient award amounts meet the mandatory minimum pass-through requirements that are applicable to SLCGP. To meet this requirement, the percentage of funds passed through to local governments must be based on the state's total SLCGP award prior to withholding any M&A.

M&A costs are for activities directly related to the management and administration of the award, such as financial management, reporting, and program and financial monitoring. Some examples of M&A costs include grants management training for M&A staff, membership fees for M&A

staff, equipment and supplies for M&A staff to administer the grant award, travel costs for M&A staff to attend conferences or training related to the grant program, travel costs for the M&A staff to conduct subrecipient monitoring, contractual services to support the M&A staff with M&A activities, and auditing costs related to the grant award to the extent required or permitted by 6 USC 665g(d)(3) or 2 C.F.R. Part 200. All membership costs utilizing SLCGP funding must be approved in advance by FEMA.

Characteristics of M&A expenses can include the following:

- Direct costs that are incurred to administer a particular federal award;
- Identifiable and unique to each federal award;
- Charged based on the activity performed for that particular federal award; and
- Not duplicative of the same costs that are included in the approved Indirect Cost Rate Agreement, if applicable.

#### **J. Pre-Award Costs**

Pre-award costs are allowable only with the prior written approval of DHS and as included in the award agreement. Grant writer fees are limited to \$1,500 per eligible entity per application.

To request pre-award costs, a written request must be included with the eligible entity's application and signed by the Authorized Organizational Representative (AOR) of the entity. The signed letter must outline the purposes for the pre-award costs, a detailed budget and budget narrative describing the pre-award costs from the post-award costs and a justification for the request. All pre-award and post-award costs should be included in the IJ and PW and clearly identified as such. The recipient must receive written confirmation from DHS that the expenses have been reviewed, and that DHS has determined the costs to be justified, unavoidable, and consistent with the grant's scope of work. The pre-award cost must meet the requirements of 2 C.F.R. § 200.458, which provides that the costs must be reasonable and necessary for efficient and timely performance of the grant's scope of work.

DHS may re-evaluate and disallow pre-award costs if it is later determined that the services were not properly procured or do not satisfy the requirements of 2 C.F.R. § 200.458.

#### **K. Beneficiary Eligibility**

There are no program requirements. See [Section 2](#) for additional eligibility information. This NOFO and any subsequent federal awards create no rights or causes of action for any beneficiary.

#### **L. Participant Eligibility**

There are no program requirements for Participant Eligibility. This NOFO and any subsequent federal awards create no rights or causes of action for any participant.

#### **M. Authorizing Authority**

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



**N. Appropriation Authority**

Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, Division J, Title V

**O. Budget Period**

There will be only a single budget period with the same start and end dates as the period of performance.

**P. Prohibition on Covered Equipment or Services**

Recipients, sub-recipients, and their contractors or subcontractors must comply with the prohibitions set forth in Section 889 of the [John S. McCain National Defense Authorization Act for Fiscal Year 2019](#), which restrict the purchase of covered telecommunications and surveillance equipment and services. Please see 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and [FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services](#) for more information.

**4. Application Contents and Format****A. Pre-Application, Letter of Intent, and Whitepapers**

Not applicable.

**B. Application Content and Format**

Not applicable.

All application forms are available on [Grants.gov](#) or [FEMA's SLCGP website](#).

**C. Application Components**

The following forms or information are required to be submitted via FEMA GO. The Standard Forms (SF) are also available at [Forms | Grants.gov](#).

- SF-424, Application for Federal Assistance
- Grants.gov Lobbying Form, Certification Regarding Lobbying
- SF-424A, Budget Information (Non-Construction) (submitted in the Attachments Section in FEMA GO)
- SF-424B, Standard Assurances (Non-Construction)
- SF-LLL, Disclosure of Lobbying Activities

**D. Program-Specific Required Documents and Information**

The following program-specific forms or information are required to be submitted in the Attachments Section in FEMA GO:

1. Cybersecurity Project Submissions (if applicable)
  - Investment Justifications (if submitting “to be determined”, reference Section 7.C, Application Criteria)
  - Project Worksheets (if submitting “to be determined”, reference Section 4.E, Post-Application Requirements for Successful Applicants)
2. Cybersecurity Planning Committee Membership List and Charter
3. Cybersecurity Plan (resubmissions if applicable)



### Investment Justification Form and Instructions

Each eligible entity is required to submit complete project-level information detailing how the SLCGP program objectives and goals will be met through the development, implementation, and/or revision of its Cybersecurity Plan. Project-level information should also include state or territory projects that address the requirement to conduct assessments and evaluation and to incorporate the adoption of key cybersecurity best practices. Eligible entities should consult the [CISA Cybersecurity Performance Goals](#) for their SLCGP application. IJs should not include brand names.

Only one application will be submitted by the eligible entity. Requirements for the application are listed in order of hierarchy below:

**Application level:** No less than one and no more than four IJs can be submitted with the application.

- **Objective:** Each submitted IJ must correspond to one SLCGP objective. Each SLCGP objective pursued by an applicant must include at least one project.
  - **Projects:** Project-level information will vary based on the associated SLCGP objectives and sub-objectives as outlined in the NOFO.
- **Project Worksheet:** Applicants must submit only one PW with the application. Multi-entity projects must be included as individual projects within a PW, aligned to the applicable IJ and SLCGP objectives.
  - Use the following naming convention for the IJs and PWs: [Insert name of state or territory] Objective [insert number of corresponding objectives – 1, 2, 3, or 4]. For example: “Alaska PW Objective 2” or “Alaska IJ Objective 2.”

The IJ Template is useful for the **Program Narrative** portion of the application. All IJs must provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of the IJs. Also, applicants must include a summary of the current capabilities within the applicant jurisdiction to address these threats and risks.

### Project Worksheet

The PW is useful for the **Budget Details and Budget Narrative** portion of the application. Eligible applicants must submit one PW as part of the overall application submission through FEMA GO. The PW must include information for each IJ submitted as part of the application for funding: IJ Number, Objective, Project Name, Local and/or Rural Pass-through information, etc.

The PW should be used to record all proposed projects with budget details, budget narrative, M&A costs, amount and source of cost share, etc. The POETE Solution Areas associated with the IJs and Projects should be indicated on the PW. The federal Amount and Cost Share Amount must be included for each project within the PW.

All project attribute fields must be completed for the PW to be considered complete. Information provided should primarily align to one objective to facilitate project review. If a project aligns to multiple objectives, then applicant must provide sufficient detail to determine which projects, POETE elements, and requested funds belong under which objective. The applicant may then

use the information collected in the worksheet for rapid transfer to the FEMA GO interface. Each project will be given a unique identifier as it is submitted via FEMA GO. Applicants should keep a record of the project identifiers as they will be required to report on each project using that identifier. All requested funding must be associated with specific projects.

### **Cybersecurity Project Submissions (if applicable)**

Applicants may request an exception to submitting their cybersecurity projects at the time of application. The exception request must be supported by the Cybersecurity Planning Committee.

**One IJ and one PW must be included with the application indicating “To be determined” on both forms.** The applicant may request M&A funding on the PW which will be released at the time of award.

Applicants are required to coordinate with the CISA Region staff (i.e., CISA Cybersecurity Advisor or CISA Cybersecurity State Coordinator) before submitting their IJs and PWs. Additionally, all updated Cybersecurity plans must be approved by the entity’s respective Cybersecurity Planning Committee. For information on Cybersecurity Plans and recommended areas for updates, committees, and charter, refer to the CISA website at [www.cisa.gov/cybergrants/slcgp](http://www.cisa.gov/cybergrants/slcgp).

Applicants can email questions about the completion and submission of the IJ, PW, or application requirements to [FEMA-SLCGP@fema.dhs.gov](mailto:FEMA-SLCGP@fema.dhs.gov). User guides are available for SLCGP IJs and PWs on FEMA’s [SLCGP website](http://www.fema.gov/slcgp). Additional programmatic guidance can be found at the CISA [SLCGP website](http://www.cisa.gov/slcgp).

## **E. Post-Application Requirements for Successful Applicants**

### **Cybersecurity Plan Renewals and Revisions**

One of the priority outcomes of the SLCGP is the approval of Cybersecurity Plans for each applicant. Applicants are still required to have a Cybersecurity and Infrastructure and Security Agency (CISA)-approved Cybersecurity Plan. Cybersecurity Plans are approved for two years and annually thereafter. In FY 2025, there are no additional plan requirements, but all entities with a CISA-approved Cybersecurity Plan must submit their current plan to CISA via the FEMA SLCGP inbox ([FEMA-SLCGP@fema.dhs.gov](mailto:FEMA-SLCGP@fema.dhs.gov)) no later than **January 30, 2026**.

All SLCGP recipients with a CISA-approved Cybersecurity Plan are required to do one of the following:

- Email your FEMA Preparedness Officer at [FEMA-SLCGP@fema.dhs.gov](mailto:FEMA-SLCGP@fema.dhs.gov) that your entity will continue to use the CISA-approved Cybersecurity Plan; or
- Email your entity’s revised Cybersecurity Plan, including a list of the revisions, to your FEMA Preparedness Officer at [FEMA-SLCGP@fema.dhs.gov](mailto:FEMA-SLCGP@fema.dhs.gov).
- Once the email or revised Cybersecurity Plan is received, FEMA will share that with CISA for their review and approval. FEMA will maintain records of CISA-approved plans and resubmitted plans for CISA review.

Additionally, review Appendix A, “[SLCGP Requirement Matrix](#)” for further guidance on post-application requirements.

## **5. Submission Requirements and Deadlines**

### **A. Address to Request Application Package**

Applications are processed through the FEMA GO system. To access the system, visit <https://go.fema.gov/>.

### **Steps Required to Apply for An Award Under This Program and Submit an Application:**

To apply for an award under this program, all applicants must:

- a. Apply for, update, or verify their Unique Entity Identifier (UEI) number and EIN from the Internal Revenue Service;
- b. In the application, provide an UEI number;
- c. Have an account with [login.gov](https://login.gov/);
- d. Register for, update, or verify their System for Award Management (SAM) account and ensure the account is active before submitting the application;
- e. Register in FEMA GO, add the organization to the system, and establish the AOR. The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see [FEMA GO Startup Guide and the SLCGP FEMA GO Application Guidance](#);
- f. Submit the complete application in FEMA GO using the SLCGP FEMA GO Application Process (copies can be obtained by emailing [FEMA-SLCGP@fema.dhs.gov](mailto:FEMA-SLCGP@fema.dhs.gov); and
- g. Continue to maintain an active SAM registration with current information at all times during which it has an active federal award or an application or plan under consideration by a federal awarding agency. As part of this, applicants must also provide information on an applicant's immediate and highest-level owner and subsidiaries, as well as on all predecessors that have been awarded federal contracts or federal financial assistance within the last three years, if applicable.

Per [2 C.F.R. § 25.110\(a\)\(2\)\(iv\)](#), if an applicant is experiencing exigent circumstances that prevents it from obtaining an UEI number and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible. Contact [fema-grants-news@fema.dhs.gov](mailto:fema-grants-news@fema.dhs.gov) and provide the details of the exigent circumstances.

How to Register to Apply:

General Instructions:

Registering and applying for an award under this program is a multi-step process and requires time to complete. Below are instructions for registering to apply for FEMA funds. Read the instructions carefully and prepare the requested information before beginning the registration process. Gathering the required information before starting the process will alleviate last-minute searches for required information.

**The registration process can take up to four weeks to complete.** To ensure an application meets the deadline, applicants are advised to start the required steps well in advance of their submission.

Organizations must have a UEI number, EIN, and an active SAM registration.

Obtain a UEI Number:

All entities applying for funding, including renewal funding, must have a UEI number. Applicants must enter the UEI number in the applicable data entry field on the SF-424 form. For more detailed instructions for obtaining a UEI number, refer to [SAM.gov](https://sam.gov).

#### Obtain Employer Identification Number:

In addition to having a UEI number, all entities applying for funding must provide an EIN. The EIN can be obtained from the IRS by visiting <https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online>.

#### Create a login.gov account:

Applicants must have a login.gov account in order to register with SAM or update their SAM registration. Applicants can create a login.gov account at: [https://secure.login.gov/sign\\_up/enter\\_email?request\\_id=34f19fa8-14a2-438c-8323-a62b99571fd](https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd).

Applicants only have to create a login.gov account once. For existing SAM users, use the same email address for both login.gov and SAM.gov so that the two accounts can be linked.

For more information on the login.gov requirements for SAM registration, refer to <https://www.sam.gov/SAM/pages/public/loginFAQ.jsf>.

#### Register with SAM:

In addition to having a UEI number, all organizations must register with SAM. Failure to register with SAM will prevent your organization from applying through FEMA GO. SAM registration must be renewed annually and must remain active throughout the entire grant life cycle.

For more detailed instructions for registering with SAM, refer to: [Register with SAM](#)

**Note:** Per [2 C.F.R. § 25.200](#), applicants must also provide the applicant's immediate and highest-level owner, subsidiaries, and predecessors that have been awarded federal contracts or federal financial assistance within the past three years, if applicable.

#### **Register in FEMA GO, Add the Organization to the System, and Establish the AOR:**

Applicants must register in FEMA GO and add their organization to the system. The organization's electronic business point of contact (eBiz POC) from the SAM registration may need to be involved in this step. For step-by-step instructions, see [FEMA GO Startup Guide](#).

Note: FEMA GO will support only the most recent major release of the following browsers:

- Google Chrome;
- Mozilla Firefox;
- Apple Safari; and
- Microsoft Edge.

Applicants using tablet type devices or other browsers may encounter issues with using FEMA GO.

### **B. Application Deadline**

08/15/2025 at 5:00 PM Eastern Time

### **C. Pre-Application Requirements Deadline**

Not applicable.

### **D. Post-Application Requirements Deadline**

Not applicable.

### **E. Effects of Missing the Deadline**

All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of submission and generates an electronic date/time stamp when FEMA GO successfully receives an application. The submitting AOR will receive via email the official date/time stamp and a FEMA GO tracking number to serve as proof of timely submission prior to the application deadline.

**Applicants experiencing system-related issues have until 3:00 PM ET on the date applications are due to notify FEMA.** No new system-related issues will be addressed after this deadline. Applications not received by the application submission deadline will not be accepted.

## **6. Intergovernmental Review**

### **A. Requirement Description and State Single Point of Contact**

An intergovernmental review may be required. Applicants must contact their state's [Single Point of Contact \(SPOC\)](#) to comply with the state's process under Executive Order 12372.

## **7. Application Review Information**

### **A. Threshold Criteria**

The Governor-designated SLCGP SAA is the only entity eligible to submit SLCGP applications to DHS. One or more states or territories may submit a multi-entity project. Subrecipient eligibility is detailed in Section 2A. "Eligibility" above.

### **B. Application Criteria**

#### **a. Programmatic Criteria**

FEMA will evaluate the FY 2025 SLCGP applications for completeness and applicant eligibility. CISA will evaluate the FY 2025 SLCGP applications for adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments.

#### **b. Review and Selection Process**

For eligible entities with a CISA-approved Cybersecurity Plan, Committee Membership List, and Charter, the review will include verification of the following elements:

- Eligible entities understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments;
- Eligible entities implement security protections commensurate with risk; and

- Eligible entities ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

In addition to the above, CISA will evaluate whether proposed projects are: 1) both feasible and effective at reducing the risks for which the project was designed; and 2) able to be fully completed within the four-year period of performance.

#### 1. Initial Review

All proposed investments will undergo a federal review by FEMA and CISA to verify compliance with all administrative and eligibility criteria identified in the NOFO. FEMA will conduct the federal review for compliance and the budget review of the IJ(s) and PW. FEMA will use a checklist to verify compliance with all administrative and eligibility criteria identified in the NOFO.

#### 2. Overall Review

Applicants must demonstrate how investments support closing capability gaps or sustaining capabilities. CISA will review IJ(s) and PW at both the investment and project level. The following criteria apply to the review of projects:

- Clarity: Sufficient detail to understand what the project is intending to do with grant dollars.
- Logical/Project Alignment: Alignment of the stated SLCGP objectives to the applicant's approved Cybersecurity Plan.
- Reasonableness: Costs for the items/services outlined within the project description are reasonable. Execution within the period of performance is feasible.

Projects rated as effective or promising are approved.

In addition, investments with emergency communications activities will be reviewed to verify compliance with the [SAFECOM Guidance on Emergency Communications Grants](#). FEMA and CISA will coordinate directly with the recipient on any compliance concerns and will provide technical assistance as necessary to help ensure full compliance.

#### c. Financial Integrity Criteria

Before making an award, FEMA is required to review the OMB-designated databases for applicants' eligibility and financial integrity information. This is required by the [Payment Integrity Information Act of 2019 \(Pub. L. No. 116-117, § 2 \(2020\)\)](#), [41 U.S.C. § 2313](#), and the ["Do Not Pay Initiative" \(31 U.S.C. 3354\)](#). For more details, see [2 C.F.R. § 200.206](#).

Thus, the Financial Integrity Criteria may include the following risk-based considerations of the applicant:

1. Financial stability.
2. Quality of management systems and ability to meet management standards.
3. History of performance in managing federal award.
4. Reports and findings from audits.
5. Ability to effectively implement statutory, regulatory, or other requirements.

#### **d. Supplemental Financial Integrity Criteria and Review**

Before making an award expected to exceed the simplified acquisition threshold (currently a total federal share of \$250,000) over the period of performance:

1. FEMA is required by [41 U.S.C. § 2313](#) to review or consider certain information found in SAM.gov. For details, see [2 C.F.R. § 200.206\(a\)\(2\)](#).
2. An applicant may review and comment on any information in the responsibility/qualification records available in SAM.gov.
3. Before making decisions in the risk review required by [2 C.F.R. § 200.206](#), FEMA will consider any comments by the applicant.

#### **C. Reviewers and Reviewer Selection**

FEMA and CISA Cybersecurity Program staff review all SLCGP applications as detailed in Section 7.B above. As an allocated program, there are no additional reviewers or selection process beyond completeness and eligibility reviews.

FEMA will follow all applicable statutes, rules, and requirements and will take into consideration materials accompanying the SLCGP legislation and annual appropriations acts, such as the Joint Explanatory Statement, as appropriate, in reviewing and determining recipient eligibility.

#### **D. Merit Review Process**

Not applicable. SLCGP is a formula-based grant as detailed in Section 4.B above.

#### **E. Final Selection**

Not applicable. SLCGP is a formula-based grant as detailed in Section 4.B above.

### **8. Award Notices**

#### **A. Notice of Award**

The Authorized Organization Representative should carefully read the federal award package before accepting the federal award. The federal award package includes instructions on administering the federal award, as well as terms and conditions for the award.

By submitting an application, applicants agree to comply with the prerequisites stated in this NOFO and the material terms and conditions of the federal award, should they receive an award.

DHS will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent via the grant application system to the submitting AOR.

Recipients must accept their awards no later than 60 days from the award date. Recipients shall notify DHS of their intent to accept the award and proceed with work via the FEMA GO system.

Funds will remain on hold until the recipient accepts the award via FEMA GO and all other conditions of the award have been satisfied, or until the award is otherwise rescinded. Failure to accept a grant award within the specified timeframe may result in a loss of funds.



## **B. Pass-Through Requirements**

The SLCGP SAA recipient must pass through at least 80% of the federal funds provided under the grant. With the consent of the local government, this pass-through may be in the form of in-kind services, capabilities, or activities, or a combination of funding and other services. Additionally, 25% of the federal award amount must go to rural areas. This pass-through to rural areas is a part of the overall 80% pass-through; however, it should be emphasized that 25% of the federal award amount must be passed through to rural areas. 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, see Section 2, “Eligibility” of this NOFO.

### **Documenting the Pass-Through**

1. The SLCGP SAA must make a firm written commitment to passing through grant funds or equivalent services to local government subrecipients;
2. The SLCGP SAA’s commitment must be unconditional (i.e., no contingencies for the availability of eligible entity funds);
3. There must be documentation (i.e., subgrant award document with terms and conditions) of the commitment; and
4. The award terms must be communicated to the local subrecipient.

The signatory authority of the SLCGP SAA must certify in writing to DHS that pass-through requirements have been met. **A letter of intent (or equivalent) to award funds is not considered sufficient.**

### **Rural Area Pass-Through**

As part of the 80% local government pass through requirement, in obligating funds, items, services, capabilities, and/or activities to local governments, each SLCGP SAA or multi-entity group is required to pass through at least 25% of the federal award amount to local jurisdictions within rural areas of the state or territory. 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 for the SLCGP, the eligible subrecipient must be a local government entity within a rural area (a jurisdiction with a population of less than 50,000 individuals).

The SLCGP SAA or multi-entity group may either pass through 25% of the federal funds provided under the grant; items, services, capabilities, or activities having a dollar value of at least 25% of the federal funds provided under the grant; or grant funds combined with other items, services, capabilities, or activities that have a total dollar value of at least 25% of the federal funds provided under the grant.

**Because the pass-through to rural entities is part of the overall 80% pass-through requirement to local governments, the eligible entity must obtain the consent of local governments if intending to pass through items, services, capabilities, or activities to rural areas in lieu of funding to count that dollar value as part of the overall 80% passthrough requirement (see 6 U.S.C. §665g(n)(2)(A)-(B)).** The same four criteria for pass-through to local governments also applies to the pass-through to rural areas within those local governments.



### Exceptions to the Pass-Through Requirement

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, and the United States Virgin Islands.

To exercise option one above, recipients must submit a proposed budget and budget narrative in the PW, along with a written justification outlining how the proposed costs will be used to revise the Cybersecurity Plan. Once the proposed costs and activities are reviewed by DHS, the recipient will be notified, and the funding will be released.

### Timing

After the funds have been released, FY 2025 SLCGP recipients must submit a letter to DHS signed by the Authorized Official listed on the grant award certifying that they have met the 45-day pass-through requirement and collected any signed local government consents. Local consent must be signed by the Authorized Official (or his/her designee) 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. 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 [SLCGPinfo@mail.cisa.dhs.gov](mailto:SLCGPinfo@mail.cisa.dhs.gov).

Please see below some example guidance on how the release of funds date may impact the mandatory pass-through requirement date:

Example – Project Name	FEMA-to-SAA Release of Funds Date	SAA-to-Local Government(s) 45-day Pass-Through Deadline Date	Letter Submission from SAA to CISA Due Date
Project A	April 15, 2025	May 30, 2025	NLT June 9, 2025
Project B	May 15, 2025	June 29, 2025	NLT July 9, 2025
Project C	June 15, 2025	July 30, 2025	NLT August 9, 2025

### Other Guidance and Requirements for Passing Through Items, Services, Capabilities, or Activities in Lieu of Funding

The Authorized Official of the SLCGP recipient entity must certify in writing to DHS that pass-through requirements have been met. If a state or territory wishes to pass through items, services, capabilities, or activities on a state-wide basis to all local governments and rural areas in lieu of funding, DHS recommends consulting with applicable municipal, city, county, rural area, or other local government councils or associations within the state or territory to gauge the level of interest in receiving these benefits in lieu of funding. DHS also recommends including these councils or associations in the approved Cybersecurity Planning Committees. Local consent must be signed by the Authorized Official (or his/her designee) for the local government entity

receiving statewide items, services, capabilities, or activities in lieu of funding, and the consent must specify the amount and intended use of the funds.

States must still engage individual local governments, as applicable, to obtain consent where the state wants to pass through items, services, capabilities, or activities to a particular local government in lieu of funding. Consent can be given by the individual local or tribal units of government. Additionally, consent to receive items, services, capabilities, or activities in lieu of funding does not have to be provided by all local governments within the state—consent is required only from those local subrecipients wishing to participate. If an individual unit of government does not consent to having the state retain a portion 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.

### **C. Note Regarding Pre-Award Costs**

Even if pre-award costs are allowed, beginning performance is at the applicant and/or sub-applicant's own risk.

### **D. Obligation of Funds**

Funds are obligated at time of award. FEMA will provide the federal award package to the applicant electronically via FEMA GO. Award packages include an Award Letter, Summary Award Memo, Agreement Articles, and Obligating Document. An award package notification email is sent via the grant application system to the submitting AOR.

### **E. Notification to Unsuccessful Applicants**

Unsuccessful applicants will be notified electronically through FEMA GO.

## **9. Post-Award Requirements and Administration**

### **A. Administrative and National Policy Requirements**

#### **Presidential Executive Orders**

Recipients must comply with the requirements of Presidential Executive Orders related to grants (also known as federal assistance and financial assistance), the full text of which are incorporated by reference.

In accordance with [Executive Order 14305, Restoring American Airspace Sovereignty \(June 6, 2025\)](#), and to the extent allowed by law, eligible state, local, tribal, and territorial grant recipients under this NOFO are permitted to purchase unmanned aircraft systems, otherwise known as drones, or equipment or services for the detection, tracking, or identification of drones and drone signals, consistent with the legal authorities of state, local, tribal, and territorial agencies. Recipients must comply with all applicable federal, state, and local laws and regulations, and adhere to any statutory requirements on the use of federal funds for such unmanned aircraft systems, equipment, or services.

## **Subrecipient Monitoring and Management**

Pass-through entities must comply with the requirements for subrecipient monitoring and management as set forth in 2 C.F.R. §§ 200.331-333.

### **B. DHS Standard Terms and Conditions**

A recipient under this funding opportunity must comply with the DHS Standard Terms and Conditions in effect as of the time of the federal award. The DHS Standard Terms and Conditions are available online: [DHS Standard Terms and Conditions | Homeland Security](#). For continuation awards, the terms and conditions for the initial federal award will apply unless otherwise specified in the terms and conditions of the continuation award. The specific version of the DHS Standard Terms and Conditions applicable to the federal award will be in the federal award package.

A recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at [www.dhs.gov/publication/dhs-standard-terms-and-conditions](http://www.dhs.gov/publication/dhs-standard-terms-and-conditions).

### **C. Financial Reporting Requirements**

1. Recipients must report obligations and expenditures through a federal financial report. The Federal Financial Report (FFR) form, also known as Standard Form 425 (SF-425), is available online at: [SF-425 OMB #4040-0014](#).
2. Recipients must submit the FFR quarterly throughout the period of performance (POP) as detailed below:
3. The final FFR is due within 120 calendar days after the end of the POP.

Reporting Documents	Report Due Date (No Later Than)
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30
Closeout FFR	No later than 120 days after the end of the POP

FEMA may withhold future federal awards and cash payments if the recipient does not submit timely financial reports, or the financial reports submitted demonstrate lack of progress or provide insufficient detail.

### **D. Programmatic Performance Reporting Requirements**

1. A Performance Report must be submitted annually throughout the POP. Recipients should refer to Appendix C, “[Sample Performance PPR and Sample Cyber Performance](#)

[Narrative for Progress Reporting](#)” for the Sample Performance Progress Report (PPR) and Sample Cyber Performance Narrative for examples of performance metrics and other data necessary to satisfy SLCGP programmatic reporting requirements.

2. A Performance Report must include:
  - a. Brief narrative of overall project(s) status;
  - b. Summary of project expenditures;
  - c. Description of any potential issues that may affect project completion;
  - d. Data collected for DHS performance measures;
  - e. Statement on the PPR form certifying compliance with SAFECOM requirements;
  - f. Cyber Performance Narrative with CISA-required programmatic data elements; and
  - g. The report must be signed and dated by the Authorized Official or Signatory Authority.
3. The PPR and Cyber Performance Narrative must be submitted through FEMA GO.
4. Performance Report Due Dates:
  - a. The annual PPR submission is due no later than January 30 of each year to account for the previous calendar year.

#### **E. Closeout Reporting Requirements**

Within 120 days after the end of the POP, or after an amendment has been issued to close out a federal award, recipients must submit the following:

1. The final request for payment, if applicable.
2. The final FFR.
3. The final progress report detailing all accomplishments.
4. A qualitative narrative summary of the impact of those accomplishments throughout the POP. If applicable, the recipient must include with the final progress report an inventory of all construction projects.
5. Other documents required by this NOFO, terms and conditions of the federal award, or other DHS guidance.

After DHS approves these reports, it will issue a closeout notice. The notice will indicate the POP as closed, list any remaining funds to be de-obligated, and address the record maintenance requirement. Unless a longer period applies, such as due to an audit or litigation, for equipment or real property used beyond the POP, or due to other circumstances outlined in [2 C.F.R. § 200.334](#), this maintenance requirement is three years from the date of the final FFR.

Also, pass-through entities are responsible for closing out those subawards as described in [2 C.F.R. § 200.344](#); subrecipients are still required to submit closeout materials within 90 calendar days of the subaward POP end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions in time for the recipient to submit all necessary documentation and information to DHS during the closeout of their prime award. The recipient is responsible for returning any balances of unobligated or unliquidated funds that have been drawn down that are not authorized to be retained per [2 C.F.R. § 200.344\(e\)](#).

#### **Administrative Closeout**

Administrative closeout is a mechanism for DHS to unilaterally execute closeout of an award. DHS will use available award information in lieu of final recipient reports, per [2 C.F.R. §](#)

[200.344\(h\)-\(i\)](#). It is an activity of last resort, and if DHS administratively closes an award, this may negatively impact a recipient's ability to obtain future funding.

### **Additional Reporting Requirements**

Recipients and subrecipients are required to adhere to all deadlines detailed in this NOFO as described in Appendix A, "[SLCGP Requirements Matrix](#)."

Anytime there is a change in personnel for any of the awardees and/or subrecipients, their information needs to be submitted for approval (all the previous personal information identified).

### **F. Disclosing Information per 2 C.F.R. § 180.335**

Before entering into a federal award, the applicant must notify DHS if it knows that the applicant or any of the principals (as defined at [2 C.F.R. § 180.995](#)) for the federal award:

1. Are presently excluded or disqualified;
2. Have been convicted within the preceding three years of any of the offenses listed in § 180.800(a) or had a civil judgment rendered against you for one of those offenses within that time period;
3. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, state, or local) with the commission of any of the offenses listed in § 180.800(a); or
4. Have had one or more public transactions (Federal, state, or local) terminated within the preceding three years for cause or default.

This requirement is fully described in [2 C.F.R. §180.335](#).

Additionally, [2 C.F.R. § 180.350](#) requires recipients to provide immediate notice to DHS at any time after entering a federal award if:

1. The recipient learns that either it failed to earlier disclose information as required by 2 C.F.R. § 180.335;
2. Due to changed circumstances, the applicant or any of the principals for the federal award now meet the criteria at 2 C.F.R. § 180.335 listed above.

### **G. Reporting of Matters Related to Recipient Integrity and Performance**

[Appendix XII to 2 C.F.R. Part 200](#) states the terms and conditions for recipient integrity and performance matters used for this NOFO.

If the total value of all active federal grants, cooperative agreements, and procurement contracts for a recipient exceeds \$10,000,000 at any time during the period of performance:

1. The recipient must maintain the currency of information reported in SAM.gov about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII;
2. The required reporting frequency is described in paragraph 4 of Appendix XII.

### **H. Single Audit Report**

A recipient expending \$1,000,000 or more in federal awards (as defined by [2 C.F.R. § 200.1](#)) during its fiscal year must undergo an audit. This may be either a single audit complying with [2 C.F.R. § 200.514](#) or a program-specific audit complying with [2 C.F.R. §§ 200.501](#) and [200.507](#).

Audits must follow [2 C.F.R. Part 200, Subpart F](#), 2 C.F.R. § 200.501, and the U.S. Government Accountability Office (GAO) [Generally Accepted Government Auditing Standards](#).

### **I. Monitoring and Oversight**

Per [2 C.F.R. § 200.337](#), DHS and its authorized representatives have the right of access to any records of the recipient or subrecipient pertinent to a federal award to perform audits, site visits, and any other official use. The right also includes timely and reasonable access to the recipient's or subrecipient's personnel for the purpose of interview and discussion related to such documents or the federal award in general.

Pursuant to this right and per [2 C.F.R. § 200.329](#), DHS may conduct desk reviews and make site visits to review and evaluate project accomplishments and management control systems, as well as provide any required technical assistance. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

Recipients and subrecipients who are pass-through entities are responsible for monitoring their subrecipients in a manner consistent with the terms of the federal award at 2 C.F.R. Part 200, including 2 C.F.R. § 200.332. This includes the pass-through entity's responsibility to monitor the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.

In terms of overall award management, recipient and subrecipient responsibilities include, but are not limited to the following: accounting of receipts and expenditures, cash management, maintaining adequate financial records, reporting and refunding expenditures disallowed by audits, monitoring if acting as a pass-through entity, or other assessments and reviews, and ensuring overall compliance with the terms and conditions of the award or subaward, as applicable, including the terms of 2 C.F.R. Part 200.

### **J. Program Evaluation**

[Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 \(2019\) \(Evidence Act\)](#) urges federal agencies to use program evaluation as a critical tool to learn, improve delivery, and elevate program service and delivery across the program lifecycle. Evaluation means "an assessment using systematic data collection and analysis of one or more programs, policies, and organizations intended to assess their effectiveness and efficiency." Evidence Act, § 101 (codified at 5 U.S.C. § 311). OMB A-11, Section 290 (Evaluation and Evidence-Building Activities) further outlines the standards and practices for evaluation activities. Federal agencies are required to specify any requirements for recipient participation in program evaluation activities (2 C.F.R. § 200.301). Program evaluation activities incorporated from the outset in the NOFO and program design and implementation allow recipients and agencies to meaningfully document and measure progress and achievement towards program goals and objectives, and identify program outcomes and lessons learned, as part of demonstrating recipient performance (2 C.F.R. § 200.301).

As such, recipients and subrecipients are required to participate in a Program Office (PO) or a DHS Component-led evaluation, if selected. This may be carried out by a third-party on behalf of the PO or the DHS Component. Such an evaluation may involve information collections

including but not limited to, records of the recipients; surveys, interviews, or discussions with individuals who benefit from the federal award, program operating personnel, and award recipients; and site visits or other observation of recipient activities, as specified in a DHS Component or PO-approved evaluation plan. More details about evaluation requirements may be provided in the federal award, if available at that time, or following the award as evaluation requirements are finalized. Evaluation costs incurred during the period of performance are allowable costs (either as direct or indirect) in accordance with [2 C.F.R. § 200.413](#). Recipients and subrecipients are also encouraged, but not required, to participate in any additional evaluations after the period of performance ends, although any costs incurred to participate in such evaluations are not allowable and may not be charged to the federal award.

#### **K. Additional Performance Reporting Requirements**

Not applicable.

#### **L. Termination of the Federal Award**

1. Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 sets forth a term and condition entitled “Termination of a Federal Award.” The termination provision condition listed below applies to the grant award and the term and condition in Paragraph C.XL of the FY 2025 DHS Standard Terms and Conditions, v.3 does not.
2. Termination of the Federal Award by FEMA

FEMA may terminate the federal award in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

- a. If the recipient or subrecipient fails to comply with the terms and conditions of the federal award.
- b. With the consent of the recipient, in which case FEMA and the recipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
- c. If the federal award no longer effectuates the program goals or agency priorities. Under this provision, FEMA may terminate the award for these purposes if any of the following reasons apply:
  - i. If DHS/FEMA, in its sole discretion, determines that a specific award objective is ineffective at achieving program goals as described in this NOFO;
  - ii. If DHS/FEMA, in its sole discretion, determines that an objective of the award as described in this NOFO will be ineffective at achieving program goals or agency priorities;
  - iii. If DHS/FEMA, in its sole discretion, determines that the design of the grant program is flawed relative to program goals or agency priorities;



- iv. If DHS/FEMA, in its sole discretion, determines that the grant program is not aligned to either the DHS Strategic Plan, the FEMA Strategic Plan, or successor policies or documents;
- v. If DHS/FEMA, in its sole discretion, changes or re-evaluates the goals or priorities of the grant program and determines that the award will be ineffective at achieving the updated program goals or agency priorities; or for other reasons based on program goals or agency priorities described in the termination notice provided to the recipient pursuant to 2 C.F.R. § 200.341.
- vi. If the awardee falls out of compliance with the Agency's statutory or regulatory authority, award terms and conditions, or other applicable laws.

### 3. Termination of a Subaward by the Pass-Through Entity

The pass-through entity may terminate a subaward in whole or in part for one of the following reasons identified in 2 C.F.R. § 200.340:

- a. If the subrecipient fails to comply with the terms and conditions of the federal award.
- b. With the consent of the subrecipient, in which case the pass-through entity and the subrecipient must agree upon the termination conditions. These conditions include the effective date and, in the case of partial termination, the portion to be terminated.
- c. If the pass-through entity's award has been terminated, the pass-through recipient will terminate its subawards.

### 4. Termination by the Recipient or Subrecipient

The recipient or subrecipient may terminate the federal award in whole or in part for the following reason identified in 2 C.F.R. § 200.340: Upon sending FEMA or the pass-through entity a written notification of the reasons for such termination, the effective date, and, in the case of partial termination, the portion to be terminated. However, if FEMA or the pass-through entity determines that the remaining portion of the federal award will not accomplish the purposes for which the federal award was made, FEMA or the pass-through entity may terminate the federal award in its entirety.

### 5. Impacts of Termination

- a. When FEMA terminates the federal award prior to the end of the period of performance due to the recipient's material failure to comply with the terms and conditions of the federal award, FEMA will report the termination in SAM.gov in the manner described at 2 C.F.R. § 200.340(c).
- b. When the federal award is terminated in part or its entirety, FEMA or the pass-through entity and recipient or subrecipient remain responsible for compliance with the requirements in 2 C.F.R. §§ 200.344 and 200.345.



## 6. Notification Requirements

FEMA or the pass-through entity must provide written notice of the termination in a manner consistent with 2 C.F.R. § 200.341. The federal award will be terminated on the date of the notification unless stated otherwise in the notification.

## 7. Opportunities to Object and Appeals

Where applicable, when FEMA terminates the federal award, the written notification of termination will provide the opportunity, and describe the process, to object and provide information challenging the action, pursuant to 2 C.F.R. § 200.342.

## 8. Effects of Suspension and Termination

The allowability of costs to the recipient or subrecipient resulting from financial obligations incurred by the recipient or subrecipient during a suspension or after the termination of a federal award are subject to 2 C.F.R. 200.343.

### **M. Best Practice**

While not a requirement in the DHS Standard Terms and Conditions, as a best practice, entities receiving funds through this program should ensure that cybersecurity is integrated into the design, development, operation, and maintenance of investments that impact information technology (IT) and/ or operational technology (OT) systems. Additionally, “The recipient and subrecipient must take reasonable cybersecurity and other measures to safeguard information including protected personally identifiable information (PII) and other types of information.” 2 C.F.R. § 200.303(e).

### **N. Payment Information**

Recipients will submit payment requests in FEMA GO for FY25 awards under this program.

#### **Instructions to Grant Recipients Pursuing Payments**

FEMA reviews all grant payments and obligations to ensure allowability in accordance with [2 C.F.R. § 200.305](#). These measures ensure funds are disbursed appropriately while continuing to support and prioritize communities who rely on FEMA for assistance. Once a recipient submits a payment request, FEMA will review the request. If FEMA approves a payment, recipients will be notified by FEMA GO and the payment will be delivered pursuant to the recipients SAM.gov financial information. If FEMA disapproves a payment, FEMA will inform the recipient.

#### **Processing and Payment Timeline**

FEMA must comply with regulations governing payments to grant recipients. See [2 C.F.R. § 200.305](#). For grant recipients other than states, [2 C.F.R. § 200.305\(b\)\(3\)](#) stipulates that FEMA is to make payments on a reimbursement basis within 30 days after receipt of the payment request, unless FEMA reasonably believes the request to be improper. For state recipients, [2 C.F.R. § 200.305\(a\)](#) instructs that federal grant payments are governed by Treasury-State Cash Management Improvement Act agreements (“Treasury-State agreement”) and default procedures

codified at [31 C.F.R. Part 205](#) and Treasury Financial Manual 4A-2000, “Overall Disbursing Rules for All Federal Agencies.” See [2 C.F.R. § 200.305\(a\)](#).

Treasury-State agreements generally apply to “major federal assistance programs” that are governed by [31 C.F.R. Part 205, subpart A](#) and are identified in the Treasury-State agreement. [31 C.F.R. §§ 205.2, 205.6](#). Where a federal assistance (grant) program is not governed by subpart A, payment and funds transfers from FEMA to the state are subject to [31 C.F.R. Part 205, subpart B](#). Subpart B requires FEMA to “limit a funds transfer to a state to the minimum amounts needed by the state and must time the disbursement to be in accord with the actual, immediate cash requirements of the state in carrying out a federal assistance program or project. The timing and amount of funds transfers must be as close as is administratively feasible to a state’s actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs.” [31 C.F.R. § 205.33\(a\)](#). Nearly all FEMA grants are not “major federal assistance programs.” As a result, payments to states for those grants are subject to the “default” rules of [31 C.F.R. Part 205, subpart B](#).

If additional information is needed, a request for information will be issued by FEMA to the recipient; recipients are strongly encouraged to respond to any additional request for information inquiries within three business days. If an adequate response is not received, the request may be denied, and the entity may need to submit a new reimbursement request; this will restart the 30-day timeline.

### **Submission Process**

All non-disaster grant program reimbursement requests must be reviewed and approved by FEMA prior to drawdowns.

For all non-disaster reimbursement requests (regardless of system), please submit the following information:

1. Grant ID / Award Number
2. Total amount requested for drawdown
3. Purpose of drawdown and timeframe covered (must be within the award performance period)
4. Subrecipient Funding Details (if applicable)
  - Is funding provided directly or indirectly to a subrecipient?
    - If **no**, include statement “This grant funding is not being directed to a subrecipient.”
  - If **yes**, provide the following details:
    - The name, mission statement, and purpose of each subrecipient receiving funds, along with the amount allocated and the specific role or activity being reimbursed.
    - Whether the subrecipient’s work or mission involves supporting aliens, regardless of whether FEMA funds support such activities.
    - Whether the payment request includes an activity involving support to aliens.
    - Whether the subrecipient has any diversity, equity, and inclusion practices.
5. Supporting documentation to demonstrate that expenses are allowable, allocable, reasonable, and necessary under [2 C.F.R. Part 200](#) and in compliance with the grant’s NOFO, award terms, and applicable federal regulations.

## O. Immigration Conditions

A recipient under this funding opportunity must comply with the FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025), with the exception Paragraph C.IX (Communication and Cooperation with the Department of Homeland Security and Immigration Officials) and paragraph C.XVII(2)(a)(iii) (Anti-Discrimination Grant Award Certification regarding immigration). Paragraphs C.IX and C.XVII(2)(a)(iii) do not apply to any federal award under this funding opportunity. The FY 2025 Department of Homeland Security Standard Terms and Conditions, v. 3 (Apr. 18, 2025) are available at [www.dhs.gov/publication/dhs-standard-terms-and-conditions](http://www.dhs.gov/publication/dhs-standard-terms-and-conditions).

## **10. Other Information**

### **A. Period of Performance Extension**

Extensions to the period of performance (POP) are not allowed.

### **B. Other Information**

#### ***a. Environmental Planning and Historic Preservation Compliance***

The federal government is required to consider effects of its actions on the environment and historic properties to ensure that activities, grants, and programs funded by FEMA, comply with federal EHP laws, Executive Orders, regulations, and policies.

Recipients and subrecipients proposing projects with the potential to impact the environment or cultural resources, such as the modification or renovation of existing buildings, structures, and facilities, and/or new construction and/or replacement of buildings, structures, and facilities, must participate in the FEMA EHP review process. This includes conducting early engagement to help identify EHP resources, such as threatened or endangered species, historic properties, or communities with environmental concerns; submitting a detailed project description with supporting documentation to determine whether the proposed project has the potential to impact EHP resources; and, identifying mitigation measures and/or alternative courses of action that may lessen impacts to those resources.

FEMA is sometimes required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not in compliance with applicable EHP laws, Executive Orders, regulations, and policies. FEMA may recommend mitigation measures and/or alternative courses of action to lessen impacts to EHP resources and bring the project into EHP compliance.

EHP guidance is found at [Environmental Planning and Historic Preservation](#). The site contains links to documents identifying agency EHP responsibilities and program requirements, such as implementation of the National Environmental Policy Act and other EHP laws, regulations, and Executive Orders. DHS and FEMA EHP policy is also found in the [EHP Directive & Instruction](#).

All FEMA actions, including grants, must comply with National Flood Insurance Program (NFIP) criteria or any more restrictive federal, state, or local floodplain management standards or

building code ([44 C.F.R. § 9.11\(d\)\(6\)](#)). For actions located within or that may affect a floodplain or wetland, the following alternatives must be considered: a) no action; b) alternative locations; and c) alternative actions, including alternative actions that use natural features or nature-based solutions. Where possible, natural features and nature-based solutions shall be used. If not practicable as an alternative on their own, natural features and nature-based solutions may be incorporated into actions as minimization measures.

The GPD EHP screening form is located at

[https://www.fema.gov/sites/default/files/documents/fema\\_ehp-screening\\_form\\_ff-207-fy-21-100\\_5-26-2021.pdf](https://www.fema.gov/sites/default/files/documents/fema_ehp-screening_form_ff-207-fy-21-100_5-26-2021.pdf).

### **b. Procurement Integrity**

When purchasing under a FEMA award, recipients and subrecipients must comply with the federal procurement standards in [2 C.F.R. §§ 200.317 – 200.327](#). To assist with determining whether an action is a procurement or instead a subaward, please consult [2 C.F.R. § 200.331](#). For detailed guidance on the federal procurement standards, recipients and subrecipients should refer to various materials issued by FEMA’s Procurement Disaster Assistance Team (PDAT).

Additional resources, including an upcoming trainings schedule can be found on the PDAT Website: <https://www.fema.gov/grants/procurement>.

Under [2 CFR 200.317](#), when procuring property and services under a federal award, states (including territories) and Indian Tribes, must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states and Indian Tribes must now follow [2 CFR 200.322](#) regarding domestic preferences for procurements and [2 CFR § 200.327](#) regarding required contract provisions.

Local government and subrecipients must have and use their own documented procurement procedures that reflect applicable state, local, tribal, and territorial (SLTT) laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200.

### **Important Changes to Procurement Standards in 2 C.F.R. Part 200**

On April 22, 2024, OMB updated various parts of Title 2 of the Code of Federal Regulations, among them the procurement standards. These revisions apply to all DHS awards with a federal award date or disaster declaration date on or after October 1, 2024, unless specified otherwise. The changes include updates to the federal procurement standards, which govern how DHS award recipients and subrecipients must purchase under a DHS award.

More information on OMB’s revisions to the federal procurement standards can be found in [Purchasing Under a FEMA Award: 2024 OMB Revisions Fact Sheet](#).

### **Competition and Conflicts of Interest**

[2 C.F.R. § 200.319\(b\)](#), applicable to local government and nonprofit recipients or subrecipients, requires that contractors that develop or draft specifications, requirements statements of work, or invitations for bids or requests for proposals must be excluded from competing for such procurements. DHS considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a recipient or subrecipient develop

its grant application, project plans, or project budget. This prohibition also applies to the use of former employees to manage the grant or carry out a contract when those former employees worked on such activities while they were employees of the recipient or subrecipient.

Under this prohibition, unless the recipient or subrecipient solicits for and awards a contract covering both development and execution of specifications (or similar elements as described above), and this contract was procured in compliance with [2 C.F.R. §§ 200.317 – 200.327](#), federal funds cannot be used to pay a contractor to carry out the work if that contractor also worked on the development of those specifications. This rule applies to all contracts funded with federal grant funds, including pre-award costs, such as grant writer fees, as well as post- award costs, such as grant management fees.

In addition to organizational conflicts of interest, situations considered to be restrictive of competition include, but are not limited to:

- Placing unreasonable requirements on firms for them to qualify to do business;
- Requiring unnecessary experience and excessive bonding;
- Noncompetitive pricing practices between firms or between affiliated companies;
- Noncompetitive contracts to consultants that are on retainer contracts;
- Specifying only a “brand name” product instead of allowing “an equal” product to be offered and describing the performance or other relevant requirements of the procurement; and
- Any arbitrary action in the procurement process.

Under [2 C.F.R. § 200.318\(c\)\(1\)](#), local government and nonprofit recipients or subrecipients are required to maintain written standards of conduct covering conflicts of interest and governing the actions of their employees engaged in the selection, award, and administration of contracts. No employee, officer, or agent may participate in the selection, award, or administration of a contract supported by a federal award if he or she has a real or apparent conflict of interest. Such conflicts of interest would arise when the employee, officer, or agent, any member of his or her immediate family, his or her partner, or an organization that employs or is about to employ any of the parties indicated herein, has a financial or other interest in or a tangible personal benefit from a firm considered for a contract. The officers, employees, and agents of the recipient or subrecipient may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, the recipient or subrecipient may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The recipient’s or subrecipient’s standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents.

Under [2 C.F.R. 200.318\(c\)\(2\)](#), if the local government and nonprofit recipient or subrecipient has a parent, affiliate, or subsidiary organization that is not a SLTT government, the recipient or subrecipient must also maintain written standards of conduct covering organizational conflicts of interest. Organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the recipient or subrecipient is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization.

The recipient or subrecipient must disclose in writing any potential conflicts of interest to DHS or the pass-through entity in accordance with applicable DHS policy.

### **Supply Schedules and Purchasing Programs**

Generally, a recipient or subrecipient may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

Information about GSA programs for states, Tribal Nations, and local governments, and their instrumentalities, can be found at [Purchasing Resources and Support for State and Local Governments.pdf](#)

[Help for state, local, and tribal governments to make MAS buys | GSA](#) and <https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments>.

### **Procurement Documentation**

Per [2 C.F.R. § 200.318\(i\)](#), local government and nonprofit recipients or subrecipients are required to maintain and retain records sufficient to detail the history of procurement covering at least the rationale for the procurement method, selection of contract type, contractor selection or rejection, and the basis for the contract price. States and Indian Tribes are reminded that in order for any cost to be allowable, it must be adequately documented per [2 C.F.R. § 200.403\(g\)](#).

Examples of the types of documents that would cover this information include:

- Solicitation documentation, such as requests for quotes, invitations for bids, or requests for proposals;
- Responses to solicitations, such as quotes, bids, or proposals;
- Pre-solicitation independent cost estimates and post-solicitation cost/price analyses on file for review by federal personnel, if applicable;
- Contract documents and amendments, including required contract provisions; and
- Other documents required by federal regulations applicable at the time a grant is awarded to a recipient.

### ***c. Financial Assistance Programs for Infrastructure***

Recipients and subrecipients must comply with FEMA's implementation requirements of the Build America, Buy America Act (BABAA), which was enacted as part of the [Infrastructure Investment and Jobs Act §§ 70901-70927, Pub. L. No. 117-58 \(2021\)](#); and [Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers](#). See also [2 C.F.R. Part 184, Buy America Preferences for Infrastructure Projects](#) and [OMB Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure](#).

None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools,



equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to implement FEMA's Build America, Buy America requirements, please see [Programs and Definitions: Build America, Buy America Act | FEMA.gov](#).

### **Waivers**

When necessary, recipients (and subrecipients through their pass-through entity) may apply for, and DHS may grant, a waiver from these requirements. A waiver of the domestic content procurement preference may be granted by the awarding official if DHS determines that:

- Applying the domestic content procurement preference would be inconsistent with the public interest;
- The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality; or
- The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25%.

The process for requesting a waiver from the Buy America preference requirements can be found at: ["Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure | FEMA.gov](#).

### **Definitions**

For definitions of the key terms of the Build America, Buy America Act, visit [Programs and Definitions: Build America, Buy America Act | FEMA.gov](#).

#### ***d. Mandatory Disclosures***

The non-Federal entity or applicant for a federal award must disclose, in a timely manner, in writing to the federal awarding agency or pass-through entity all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. [2 C.F.R. § 200.113](#).

#### ***e. Adaptive Support***

Pursuant to [Section 504 of the Rehabilitation Act of 1973](#), recipients of DHS financial assistance must ensure that their programs and activities do not discriminate against qualified individuals with disabilities.

#### ***f. Record Retention***

##### **Record Retention Period**

Financial records, supporting documents, statistical records, and all other non-federal entity records pertinent to a federal award generally must be maintained for at least three years from the date the final FFR is submitted. See [2 C.F.R. § 200.334](#). Further, if the recipient does not submit

a final FFR and the award is administratively closed, DHS uses the date of administrative closeout as the start of the general record retention period. The record retention period **may be longer than three years or have a different start date** in certain cases.

### **Types of Records to Retain**

DHS requires that recipients and subrecipients maintain the following documentation for federally funded purchases:

- Specifications;
- Solicitations;
- Competitive quotes or proposals;
- Basis for selection decisions;
- Purchase orders;
- Contracts;
- Invoices; and
- Cancelled checks.

### ***Actions to Address Noncompliance***

Non-federal entities receiving financial assistance funding from DHS are required to comply with requirements in the terms and conditions of their awards or subawards, including the terms set forth in applicable federal statutes, regulations, NOFOs, and policies. Throughout the award lifecycle or even after an award has been closed, DHS or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient.

In the case of any potential or actual noncompliance, DHS may place special conditions on an award per [2 C.F.R. §§ 200.208](#) and [200.339](#). DHS may place a hold on funds until the matter is corrected, or additional information is provided per [2 C.F.R. § 200.339](#), or it may do both. Similar remedies for noncompliance with certain federal civil rights laws are authorized pursuant to [44 C.F.R. Part 7](#) and [44 C.F.R. Part 19](#) or other applicable regulations.

If the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, DHS may take other remedies allowed under [2 C.F.R. § 200.339](#).

### ***g. Audits***

FEMA grant recipients are subject to audit oversight from multiple entities including the DHS OIG, the GAO, the pass-through entity, or independent auditing firms for single audits, and may cover activities and costs incurred under the award. Auditing agencies such as the DHS OIG, the GAO, and the pass-through entity (if applicable), and FEMA in its oversight capacity, must have access to records pertaining to the FEMA award.



### **11. Appendix A: SLCGP Requirements Matrix**

ID	Category	Requirement	Location	Due Date Cycle	Due Date	Submission Plan
1	Administrative	Pass-through Requirement	NOFO, Sec. 8	Within 45 calendar days of release of funds	Varies	Email Certification letter in writing to FEMA
2	Administrative	Rural Pass-through Requirements	NOFO Sec. 8	Within 45 Calendar days of release of funds	Varies	Email Certification letter in writing to FEMA
3	Application	Cybersecurity Plan (Resubmissions, if applicable, required by January 30, 2026)	NOFO Sec. 3	Prior to award or during POP (if not already approved by CISA)	Varies	Pre-Award-: FEMA GO Post Award: Submit by email to FEMA (Password Protected)
4	Application	Cybersecurity Planning Committee Membership List	NOFO Sec. 3	Prior to award or during POP (if not already approved by CISA)	Varies	Prior to Award: FEMA GO Post Award: Submit to FEMA (Password Protected)
5	Application	Cybersecurity Planning Committee Charter	NOFO Sec. 3	Prior to award or during POP (if not already approved by CISA)	Varies	Pre-Award: FEMA GO Post Award: Submit to FEMA (Password Protected)
6	Application	Investment Justification	NOFO Sec. 4	Prior to award	At time of application	Pre-Award: FEMA GO Post Award: Submit to FEMA
7	Application	Project Worksheet	NOFO Sec. 4	Prior to award	At time of application	Pre- Award: FEMA GO Post Award: Submit to FEMA
8	Financial Closeout	Financial Closeout Reporting Requirements	NOFO Sec. 9	Within 120 days after end of POP	Varies	Submit final SF-425 Federal Financial Report (FFR) in the Payment and Reporting Systems (PARS); process final reimbursement requests in PARS
9	Cost Share	Cost Share Requirement	NOFO Sec 2, 4	Application, Quarterly, Closeout	Varies	FFR/SF-425 (Quarterly and at Closeout)
10	Exercises	EHP Review/ Approval	NOFO Sec. 10	Prior to conducting exercises that require EHP Review as outlined in NOFO Section F.	Varies	Email to: GPDEHPInfo@fema.dhs.gov and cc: FEMA-SLCGP@fema.dhs.gov
11	Administrative	Minor Modifications	NOFO Sec. 3	Prior to conducting any minor modifications projects as outlined in NOFO Section 3G.	Varies	Email to: GPDEHPInfo@fema.dhs.gov and cc: FEMA-SLCGP@fema.dhs.gov

ID	Category	Requirement	Location	Due Date Cycle	Due Date	Submission Plan
12	Procurement	Build America, Buy America Act	NOFO Sec. 10	Throughout POP	Varies	N/A
13	Pre-Award	Pre-award Cost	NOFO Sec. 3	Pre-award (if applicable)	At time of application	Written request included with the eligible entity's application and signed by the AOR of the entity. Letter must be submitted with the PW and IJ via FEMA GO
14	Post Award	Cybersecurity Membership (Cyber Hygiene Services)	NOFO Appendix B	Post award	During the first year of the award/ subaward POP, and annually	Required for SAAs and their subrecipients, as well as all entities receiving non-funding services, benefits, etc. in lieu of funding.
15	Reporting	SF-425, also known as the FFR	NOFO Sec. 9	Quarterly	30-Jan 30-Apr 30-Jul 30-Oct	Submit SF-425 FFR in the PARS
16	Progress Reporting and Performance Measurement	Performance Progress Report and Cyber Performance Narrative	NOFO Sec. 9	Once annually and at Closeout	30-Jan and Closeout	Submit signed SF-PPR Report (PDF) and a Cyber Performance Narrative (Samples of both reports can be found in the Appendix C). Recipients should include compliance with the SAFECOM Guidance on the SF-PPR report.
17	Reporting	Single Audit Report	NOFO Sec. 9	Throughout POP	Varies	<a href="#">Federal Audit Clearinghouse</a>

## **12. Appendix B: Required, Encouraged, and Optional Services, Memberships, and Resources**

All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA with specific requirements depending upon the entity and type of funding received. Cyber Hygiene services are required for all SLCGP recipients, subrecipients, and entities receiving the benefits of services, activities, etc., in lieu of funding. For these required services and memberships, note that participation is not required for submission and approval of a grant but is a post-award requirement.

### **Required Services**

<b>Services &amp; Memberships</b>	<b>State government must enroll/complete?</b>	<b>Local government must enroll/complete?</b>	<b>Local or state government must enroll/complete if it receiving benefits, services, etc. in lieu of funding?</b>
Cyber Hygiene services, specifically: Vulnerability Scanning	Required	Required	Required

### **Cyber Hygiene Services**

Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static Internet Protocols for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for this service, email [vulnerability@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov) with the subject line “Requesting Cyber Hygiene Services – SLCGP” to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP. For more information, visit CISA’s [Cyber Hygiene Information web page](#).

### **CISA Recommended Resources, Assessments, and Memberships (not mandatory)**

The following list of CISA resources are recommended products, services, and tools provided at no cost to federal and SLT governments, as well as public and private sector critical infrastructure organizations:

- [Cyber Resource Hub](#)
- [Ransomware Guide \(Sept. 2020\)](#)
- [Cyber Resilience Review](#)
- [External Dependencies Management \(EDM\) Assessment](#)
- [EDM Downloadable Resources](#)
- [Cyber Infrastructure Survey](#)
- [Free Public and Private Sector Cybersecurity Tools and Services](#)
- [Cross-Sector Cybersecurity Performance Goals](#)
- [Information Technology \(IT\) Sector-Specific Goals \(SSGs\) | CISA](#)
- [Web Application Scanning](#)

- [Risk and Vulnerability Assessments - Penetration Testing](#)
- [Cyber Resilience Essentials Assessment](#)
- [CISA's Cybersecurity Marketplace](#)
- [Known Exploited Vulnerabilities Catalog](#)

In addition to these resources, CISA's [Interoperable Communications Technical Assistance Program](#) (ICTAP) provides direct support to SLT emergency responders and government officials across all 56 states and territories through training, tools, and onsite assistance to advance public safety interoperable communications capabilities. These services are provided at no cost and scalable to the community's needs. Within the catalog, the 9-1-1/Public Safety Answering Point/Land Mobile Radio Cyber Assessment technical assistance offering provides organizations with a review of their cyber posture in accordance with nationally recognized best practices guidelines. CISA employs the NIST Special Publication 800-53, Rev 5, "Security and Privacy Controls for Information Systems and Organizations" as a framework. Requests for ICTAP assistance are coordinated through the [Statewide Interoperability Coordinator](#) from each state and territory.

CISA Central: To report a cybersecurity incident, visit <https://www.us-cert.gov/report>. For additional CISA services, visit the [CISA Services Catalog](#).

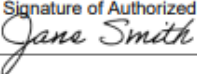
[All Resources & Tools | CISA](#) allows users to filter by audience (e.g., state, local, tribal, and territorial government or educational institutions) when browsing available resources.

For additional information on memberships, visit [Information Sharing and Analysis Organization \(ISAO\) Standards Organization](#). All membership costs utilizing SLCGP funding must be approved in advance by FEMA.

### **13. Appendix C: Sample Performance Progress Report (PPR) and Sample Cyber Performance Narrative for Progress Reporting**

The Sample PPR and Sample Cyber Performance Narrative on the following pages include examples of performance metrics and other data necessary to satisfy SLCGP programmatic reporting requirements. Grant recipients are encouraged to use these samples and the instructions therein to prepare and submit annual progress reporting data for SLCGP awards.

**PERFORMANCE PROGRESS REPORT  
SF-PPR**

		Page	of Pages
1. Federal Agency and Organization Element to Which Report is Submitted Federal Emergency Management Agency		2. Federal Grant or Other Identifying Number Assigned by Federal Agency EMW-2025-CY-12345	
		3a. DUNS Number 123456789	
		3b. EIN 123456789	
4. Recipient Organization (Name and complete address including zip code) HappyLand Emergency Management Agency 1234 Happy St. Land, U.S.A. 00000		5. Recipient Identifying Number or Account Number	
6. Project/Grant Period Start Date: (Month, Day, Year)      End Date: (Month, Day, Year)		7. Reporting Period End Date (Month, Day, Year)	
12/01/2025      11/30/2029		12/31/2026	
		8. Final Report? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
		9. Report Frequency <input checked="" type="checkbox"/> annual <input type="checkbox"/> semi-annual <input type="checkbox"/> quarterly <input type="checkbox"/> other (If other, describe: _____)	
10. Performance Narrative (attach performance narrative as instructed by the awarding Federal Agency) Federal Award Amount - \$1,234,567; Cost Share (0%) - Recipient has approved cost share waiver Total Federal Funding for Management and Administration (5% M&A) - \$61,728.35 Total Federal Funding for Projects - \$612,000 Total Federal Funding "To Be Determined" for Projects - \$560,838.65 Expended to date and drawdown Federal Funding for Projects Only - \$55,249.25 Expended to date and drawdown Federal Funding for M&A Only - \$35,000.00 Total Federal Funding Expended to Date: \$90,249.25 Remaining Balance of Federal Funding for Projects Only - \$556,750.75 Remaining Balance of Federal Funding for M&A - \$26,728.35 Remaining Balance of Federal Funding "To Be Determined" for Projects - \$560,838.65 Remaining Federal Funding Balance - \$1,144,317.75  Statewide Cybersecurity Plan approved by FEMA/CISA. The recipient certifies that all of the grant funding used to support emergency communications investments will comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). The recipient's conformance with the SAFECOM Guidance ensures that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. See attachment for performance narrative.			
11. Other Attachments (attach other documents as needed or as instructed by the awarding Federal Agency)			
12. Certification: I certify to the best of my knowledge and belief that this report is correct and complete for performance of activities for the purposes set forth in the award documents.			
12a. Typed or Printed Name and Title of Authorized Certifying Official Ms. Jane Smith, Director		12c. Telephone (area code, number and extension) 1-234-567-890	
		12d. Email Address happyland@ema.gov	
12b. Signature of Authorized Certifying Official 		12e. Date Report Submitted (Month, Day, Year) 1/30/26	
		13. Agency use only	

FY 2025 SLCGP Performance Narrative: HappyLand EMA

## FY 2025 SCLGP Performance Narrative: HappyLand Emergency Management Agency (EMA)

### Narrative of Overall Projects Status

*Insert a narrative of the overall project status in this section.*

### HappyLand EMA Project Expenditures

The State of HappyLand has 4 CISA-approved projects, obligating \$612,000 in Federal funds with \$55,249.25 total expenditures to date for approved project funding only. CISA-approved projects include the following:

Project Name as detailed on approved Project Worksheet:	Expenditures to date:
Town of Columbia Endpoint Detection Project	\$87,000
University of XXX Cybersecurity Training Course for Local Jurisdictions Project	\$300,000
State XXX CISO Firewall Upgrade Project	\$150,000
Central Community College Cyber Risk Assessment Project	\$75,000

**Note:** Another option for reporting the expenditure-to-date and remaining balance information per project is to add a column to the CISA-approved Project Worksheet and providing that with the PPR submission.

## HappyLand EMA Cybersecurity Plan Metrics

Project Objectives	Program Sub-Objectives	Associated Metrics	Metric Description
1. Implement a centralized cybersecurity governance structure, policies, processes and baseline measures to build and maintain cyber resiliency across the state.	1.1 Develop and institutionalize the state's cybersecurity framework based on the NIST CSF.	80%  Percentage of local government entities which have implemented the cybersecurity framework based on their individual risk profile.	The total number of local government entities which have implemented the cybersecurity framework by the total number of local government entities responding to a request for that information.

## HappyLand EMA Performance Measures

**Performance metrics vary across the fiscal years and programs (SLCGP or TCGP).** Recipients should ensure they are using the **correct** performance measures for their submitted performance narratives. The specific measures can be found in the NOFOs linked below:

- [FY 2022 SLCGP](#)
- [FY 2023 SLCGP](#) and [FY 2023 TCGP](#)
- [FY 2024 SLCGP](#)
- FY 2025 SLCGP and FY 2025 TCGP

The chart below is a sample of how a recipient would complete the performance measures using the **FY 2025 SLCGP NOFO** requirements for Performance Measures (3E).

**Responses for Performance Measure as requesting "Percentage of" should either be "100%" for completed status or "0" for incomplete/in progress status. Metrics should be answered on behalf of your SLCGP program to CISA as "Entities" equals State or Territory. When the metric value is zero, responses should be entered as "0."**



Performance Measure	Quantified Metric
Percentage of entities conducting annual tabletop and full-scale exercises to test Cybersecurity Plans (40% target range).	100%
Amount of grant funds budgeted for cybersecurity exercises (10% target range).	100%
Percentage of grant funds expended on exercise plans for entities (10% target range).	100%
Percentage of entities conducting annual cyber risk assessments conducted to identify cyber risk management gaps and areas for improvement (80% target range).	100%
Percentage of entities performing phishing training (70% target range).	0
Percentage of entities conducting awareness campaigns (90% target range).	100%
Percentage of entities providing role-based cybersecurity awareness training (90% target range).	0
Percentage of entities with capabilities to analyze network traffic and activities related to potential threats (60% target range).	0
Percentage of entities implementing multi-factor authentication (MFA) for all remote access and privileged accounts (70% target range).	100%
Percentage of entities with programs to anticipate and discontinue end-of-life software and hardware (90% target range).	0
Percentage of entities prohibiting the use of known/fixed/default passwords and credentials (90% target range).	100%
Percentage of entities operating under the ".gov" internet domain (70% target range).	100%
Percentage of entities that reported CISA-identified Cybersecurity Gaps (50% target range).	0
Percentage of entities with Endpoint Detection Response systems that were funded for implementation (90% target range).	100%
Number of capabilities ratings improved (50% target range).	100%
Percentage of state/territory-created performance metrics that were met (50% target range).	100%

Performance Measure	Quantified Metric
Percentage of entities participating in CISA services (50% target range).	0
Percentage of entities that have implemented data encryption projects (50% target range).	0
Percentage of entities that have implemented enhanced logging projects (60% target range).	0
Percentage of entities that have implemented system reconstitution projects (60% target range).	100%

## State- or Territory-specific Performance Metrics

Recipients may report in the table below any meaningful progress made on SLGGP-funded or TCGP-funded projects.

Performance Measures	Quantified Metric

## Description of Potential Issues

- *We anticipate no issues with completing all approved projects within the period of performance.*

## **14. Appendix D: POETE Solution Areas for Investments**

### **Overview**

Funding guidelines established within this section support developing, updating, and implementing a Cybersecurity Plan. Allowable investments made in support of this program must fall into the categories of POETE, aligned to closing capability gaps or sustaining capabilities. Additionally, FEMA and CISA published Information Bulletin No. 523, “[FEMA SLCGP Minor Modifications to Facilities](#)” in December 2024, describing allowable costs for minor modifications to facilities.

### **Guidance**

Section 2220A(n)(6) of the *Homeland Security Act of 2002* (codified as amended at 6 U.S.C. § 665g(n)(6)) prohibits recipients and subrecipients under the SLCGP and Tribal Cybersecurity Grant Program (TCGP) from using a “grant awarded...to construct, remodel, or perform alterations of buildings and other physical facilities.” However, this section does not prohibit a recipient or subrecipient from making a minor modification to an existing building or other physical facility necessary to install and connect equipment purchased under a grant award or subaward, such as drilling a hole in a building’s wall to mount that equipment. In addition, the prohibition under Section 2220A(n)(6) does not apply in circumstances where a recipient or subrecipient constructs, remodels or performs alterations of buildings or other physical facilities with its own funding when installing and connecting equipment for an information system purchased under a grant award or subaward. The prohibition under Section 2220A(n)(6) only applies to work and associated costs sourced with federal funding and/or the nonfederal share of a grant award and does not apply to work completed at a recipient’s or subrecipient’s own expense.

Recipients and subrecipients may use SLCGP funding to perform minor modifications that **do not** substantially affect a building’s, or other physical facility’s, structure, layout or systems; affect critical aspects of a building’s safety; or otherwise materially increase the value or useful life of the building or other physical facility. The prohibition would also apply to the nonfederal cost-sharing requirement detailed in Section 2220A(m) (codified as amended at 6 U.S.C. § 665g(m)). As a reminder, all projects and associated budgets must support the approved Cybersecurity Plan and be approved in advance by the Cybersecurity and Infrastructure Security Agency and FEMA.

Examples of the types of minor modifications that could be **allowable** with SLCGP funding, and the non-federal cost share, are listed below:

- Fastening equipment to building or other physical facility walls where it does not become a permanent fixture (such as hanging a server rack with servers on a building wall).
- Replacing an outdated existing electrical or internet outlet into which the equipment will connect.
- Installing new cabling.
- Replacing existing cabling.
- Moving cabling.

- Installing and connecting information system equipment to the building's network and power supply and internet.
- Making a hole in the wall to attach the equipment to the building's network, power or internet.

Unallowable remodeling and alterations include permanent modifications that substantially affect the building's, or other physical facility's, structure, layout or systems; affect critical aspects of a building's or other physical facility's safety (such as structural integrity and fire safety systems); or other modifications that materially increase the value or useful life of the building or other physical facility.

Examples of the types of construction, remodeling and alterations that are **unallowable** with SLCGP funding, or the non-federal cost share, are listed below:

- Constructing a new building or other physical facility.
- Updating an electrical system to a building or other physical facility that involves work to enhance or modernize the electrical infrastructure, such as replacing electrical panels, upgrading old or unsafe wiring, and replacing circuit breakers.
- Installing new walls or reconfiguring existing walls.
- Affixing equipment in such a way that it becomes a permanent part of a building or other physical facility (as this would result in the equipment no longer being personal property).

Because Section 2220A(n)(6) does not apply to minor modifications that do not: substantially affect a building or other physical facility's structure, layout, or systems; affect critical aspects of a building or other physical facility's safety; or otherwise materially increase the value or useful life of a building or other physical facility, minor modifications **may be permitted under the SLCGP subject to additional reviews**. As a reminder, recipients (and subrecipients through the State Administrative Agency) are required to submit projects for minor building modifications approval to the FEMA Grant Programs Directorate Environmental Planning and Historic Preservation Branch. Questions regarding this requirement may be directed to [SLCGPinfo@mail.cisa.dhs.gov](mailto:SLCGPinfo@mail.cisa.dhs.gov).

## Planning

Planning costs are allowable under this program. SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of the holistic, entity-wide Cybersecurity Plan and other planning activities that support the program goals and objectives and Cybersecurity Planning Committee requirements. **FEMA will not release funds to a recipient until CISA approves the entity's Cybersecurity Plan.** Planning activities may include the following:

- Update or revision of statewide Cybersecurity Plan;
- Cybersecurity incident response plans or planning; and
- Business continuity and/or disaster recovery plans.

## Organization

Organization costs are allowable under this program. States and territories must justify proposed expenditures of SLCGP funds to support organization activities within their Investment Justifications and Project Worksheet submissions. Organizational activities may include the following:

- Program management;
- Development of whole community partnerships that support the approved Cybersecurity Planning Committee;
- Structures and mechanisms for information sharing between the public and private sector; and
- Operational support.

Personnel hiring, overtime, and backfill expenses are permitted under this grant to perform allowable SLCGP POETE activities. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and cybersecurity navigators. The grant recipient must demonstrate that the personnel will be sustainable once the program ends or funds are no longer available.

## Equipment

Equipment costs are allowable under this program. SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLT governments.

Recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable [SAFECON Guidance on Emergency Communications Grants](#) recommendations. Such investments must be coordinated with the Statewide Inoperability Coordinator (SWIC) and the State Interoperability Governing Body (SIGB) to ensure interoperability and long-term compatibility.

SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. These contracts may exceed the period of performance if they are purchased incidental to the original purchase of the system or equipment, as long as the original purchase of the system or equipment is consistent with that which is typically provided for, or available through, these types of agreements, warranties, or contracts.

When purchasing a stand-alone warranty or extending an existing maintenance contract on a system or an already-owned piece of equipment, coverage purchased may not exceed the period of performance of the award used to purchase the maintenance agreement or warranty, and it may only cover equipment purchased with SLCGP funds or for equipment dedicated for SLCGP-related purposes. As with warranties and maintenance agreements, this extends to licenses and user fees as well.

The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted. Except for maintenance plans or extended warranties purchased incidental to the original purchase of the equipment, the period covered by maintenance or warranty plan must not exceed the period of performance of the specific grant funds used to purchase the plan or warranty.

## Training

Training costs are allowable under this program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the eligible entity's approved Cybersecurity Plan, address a performance gap identified through assessments, and contribute to building a capability that will be evaluated through a formal exercise. Recipients are encouraged to use existing training rather than developing new courses. When developing new courses, recipients are encouraged to apply the Analyze, Design, Develop, Implement, and Evaluate model of instructional design.

Recipients are also encouraged to use FEMA's [National Preparedness Course Catalog](#). Trainings include programs or courses developed for and delivered by institutions and organizations funded by FEMA. This includes the Center for Domestic Preparedness, the Emergency Management Institute, and FEMA's Training Partner Programs, including the Continuing Training Grants, the National Domestic Preparedness Consortium, the Rural Domestic Preparedness Consortium, and other partners. The catalog features a wide range of course topics in multiple delivery modes to meet FEMA's mission scope as well as the increasing training needs of federal, state, local, and territorial audiences.

Some training activities require Environmental and Historic Preservation (EHP) Review, including exercises, drills, or **trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises**. Additional information on training requirements and EHP review can be found online at [Environmental Planning and Historic Preservation | FEMA.gov](#).

CISA's Federal Virtual Training Environment offers cybersecurity training to federal, state, local, tribal, and territorial government employees, which offer education and certifications aligned with the NICE Workforce Framework for Cybersecurity. Additional information can be found at [CISA Learning | National Institute for Cybersecurity Careers and Studies](#).

## Exercises

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at [HSEEP | FEMA.gov](#).

Some exercise activities require EHP review, including exercises, drills, or trainings that require any type of land, water, or vegetation disturbance or building of temporary structures or that are not located at facilities designed to conduct training and exercises. Additional information on exercise requirements and EHP review can be found online at [Environmental Planning and Historic Preservation | FEMA.gov](#).