

**The U. S. Department of Homeland Security (DHS)
Notice of Funding Opportunity (NOFO)
Fiscal Year 2024 State and Local Cybersecurity Grant Program**

All entities wishing to do business with the federal government must have a unique entity identifier (UEI). The UEI number is issued by the system. Requesting a UEI using System for Award Management (SAM.gov) can be found at: <https://sam.gov/content/entity-registration>.

Grants.gov registration information can be found at: <https://www.grants.gov/register>

Updates in Grant Application Forms:

The Data Universal Numbering System (DUNS) Number was replaced by a new, non-proprietary identifier requested in, and assigned by SAM.gov. This new identifier is the Unique Entity Identifier.

Additional Information can be found on Grants.gov: <https://www.grants.gov/forms/forms-development/planned-uei-updates>.

Table of Contents

Updates in Grant Application Forms:	1
A. Program Description	6
1. Issued By	6
2. Assistance Listings Number	6
3. Assistance Listings Title	6
4. Funding Opportunity Title	6
5. Funding Opportunity Number	6
6. Authorizing Authority for Program	6
7. Appropriation Authority for Program	6
8. Announcement Type	6
9. Program Category	6
10. Program Overview, Objectives, and Priorities	6
a. Overview	6
b. Goals, Objectives, and Priorities	7
c. Alignment to Program Purpose and the DHS and FEMA Strategic Plan	11
11. Performance Measures	12
B. Federal Award Information	13
1. Available Funding for the NOFO: \$279,873,562	13
2. Projected Number of Awards: 56	15
3. Period of Performance: 48 months	15
4. Projected Period of Performance Start Date: 2/01/2025	15
5. Projected Period of Performance End Date: 1/31/2029	15
6. Funding Instrument Type: Grant	15
C. Eligibility Information	15
1. Eligible Applicants	15
2. Applicant Eligibility Criteria	15
3. Subawards and Beneficiaries	15
a. Subaward Allowability	15
b. Subrecipient Eligibility	16
c. Other Subaward Information: Public Educational Institutions	16
d. Beneficiaries or Participants	16
4. Other Eligibility Criteria/Restrictions	16
5. Cost Share or Match	17
a. Types of Cost Share/Match	17
b. Cost Share Documentation	18
c. Calculating Cost Share for the Application	18
d. Calculating Cost Share for Projects	19
e. Future Cost Share Amounts	19
f. Cost Share Waiver	19
D. Application and Submission Information	21
1. Key Dates and Times	21
a. Application Start Date: 09/23/2024 at 9:00 AM ET	21
b. Application Submission Deadline: 12/3/2024 at 5:00 PM ET	21
c. Anticipated Award Date: No later than 02/01/2024	22
d. Other Key Dates	22

2.	Agreeing to Terms and Conditions of the Award	22
3.	Address to Request Application Package	22
4.	Requirements: Obtain a Unique Entity Identifier (UEI) and Register in the System for Award Management (SAM.gov)	22
5.	Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application	23
6.	Electronic Delivery	24
7.	How to Register to Apply	24
	a. General Instructions:	24
	b. Obtain an UEI Number:	24
	c. Obtain Employer Identification Number	24
	d. Create a login.gov account:	25
	e. Register with SAM:	25
	f. Register in FEMA GO, Add the Organization to the System, and Establish the AOR:	26
8.	Submitting the Application	26
9.	Timely Receipt Requirements and Proof of Timely Submission	26
10.	Content and Form of Application Submission	27
	a. Standard Required Application Forms and Information	27
	b. Program-Specific Required Forms and Information	27
11.	Other Submission Requirements	29
12.	Intergovernmental Review	29
13.	Funding Restrictions and Allowable Costs	29
	a. Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services	30
	b. Pre-Award Costs	31
	c. Management and Administration (M&A) Costs	32
	d. Indirect Facilities & Administrative (F&A) Costs	32
	e. Evaluation Costs	33
	f. Other Direct Costs	33
E.	Application Review Information	34
	1. Application Evaluation Criteria	34
	a. Programmatic Criteria	34
	b. Financial Integrity Criteria	34
	c. Supplemental Financial Integrity Criteria and Review	34
	2. Review and Selection Process	35
F.	Federal Award Administration Information	36
	1. Notice of Award	36
	2. Pass-Through Requirements	36
	a. Documenting the Pass-Through	36
	b. Rural Area Pass-Through	36
	c. Exceptions to the Pass-Through Requirement	37
	d. Timing	37
	e. Other Guidance and Requirements for Passing Through Items, Services, Capabilities, or Activities in Lieu of Funding	37
	3. Administrative and National Policy Requirements	38

a.	DHS Standard Terms and Conditions	38
b.	Ensuring the Protection of Civil Rights	38
c.	Environmental Planning and Historic Preservation (EHP) Compliance	38
d.	SAFECOM Guidance Compliance	38
e.	Requirement for Using CISA Services	38
f.	Mandatory Disclosures	38
e.	Uniform Administrative Requirements, Cost Principles, and Audit Requirements..	38
4.	Reporting.....	38
a.	Financial Reporting Requirements	38
b.	Programmatic Performance Reporting Requirements.....	39
c.	Closeout Reporting Requirements.....	39
d.	Additional Reporting Requirements.....	41
5.	Monitoring and Oversight.....	42
G.	DHS Awarding Agency Contact Information.....	44
1.	Contact and Resource Information	44
a.	FEMA Program Office Contact	44
b.	CISA Grant Program Office Contact	44
c.	FEMA Grants News	44
d.	Grant Programs Directorate (GPD) Award Administration Division	44
e.	Equal Rights	44
f.	Environmental Planning and Historic Preservation	45
2.	Systems Information	45
a.	FEMA GO	45
H.	Additional Information.....	45
1.	Termination Provisions.....	45
a.	Noncompliance.....	45
b.	With the Consent of the Recipient	45
c.	Notification by the Recipient	46
2.	Program Evaluation	46
3.	Period of Performance Extensions.....	46
4.	Disability Integration	47
5.	Conflicts of Interest in the Administration of Federal Awards or Subawards.....	48
6.	Procurement Integrity	49
a.	Important Changes to Procurement Standards in 2 C.F.R. Part 200	49
b.	Competition and Conflicts of Interest	50
c.	Supply Schedules and Purchasing Programs.....	52
d.	Procurement Documentation.....	53
7.	Financial Assistance Programs for Infrastructure.....	53
a.	Build America, Buy America Act	53
b.	Waivers.....	54
c.	Definitions	55
8.	Record Retention	55
a.	Record Retention Period	55
b.	Types of Records to Retain	56
9.	Actions to Address Noncompliance.....	56
10.	Audits.....	57

11. Payment Information	59
12. Whole Community Preparedness.....	59
13. Report issues of fraud, waste, abuse	59
14. Continuity Capability	59
15. Hazard-Resistant Building Codes	60
16. Appendices.....	60
Appendix A: Program Goals and Objectives.....	1
Appendix B: Cybersecurity Planning Committee and Charter.....	1
Appendix C: Cybersecurity Plan	1
Appendix D: POETE Solution Areas for Investments	1
Appendix E. SLCGP Requirements Matrix.....	1
Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources	1

A. Program Description

1. Issued By

U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Grant Programs Directorate (GPD)

2. Assistance Listings Number

97.137

3. Assistance Listings Title

State and Local Cybersecurity Grant Program

4. Funding Opportunity Title

Fiscal Year 2024 State and Local Cybersecurity Grant Program (SLCGP)

5. Funding Opportunity Number

DHS-24-GPD-137-00-99

6. Authorizing Authority for Program

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

7. Appropriation Authority for Program

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

8. Announcement Type

Initial

9. Program Category

Preparedness: Infrastructure Security

10. Program Overview, Objectives, and Priorities

a. Overview

Our nation faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities in critical infrastructure.

Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of state, local, and territorial (SLT) governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (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 strengthen the security of critical infrastructure and improve the resilience of services SLT governments provide their communities.

b. Goals, Objectives, and Priorities

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.

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 Appendix A, “[Program Goals and Objectives](#)” for more information on SLCGP program goals, objectives, sub-objectives, and desired outcomes required in their Fiscal Year (FY) 2024 SLCGP application.

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:

- Establish a Cybersecurity Planning Committee;
- 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.

For those states that did not apply for FY 2022 or FY 2023 SLCGP funding, or for FY 2022 SLCGP recipients that were unable to meet the requirements listed above, please refer to Appendix A, “[Program Goals and Objectives](#)” and Appendix B, “[Cybersecurity Planning Committee and Charter](#)” for more information on the FY 2022 requirements that must be met before development of applications for FY 2024.

Cybersecurity Plan Renewals and Revisions

All applicants with a Cybersecurity and Infrastructure Security Agency (CISA) approved Cybersecurity Plan must submit their current Cybersecurity Plan to CISA via the FEMA SLCGP Inbox at FEMA-SLCGP@fema.dhs.gov no later than **January 30, 2025**, and annually thereafter on the same date throughout the grant's period of performance. When submitting a Cybersecurity Plan, applicants must inform CISA if they revised their plan since CISA's last approval of it. If the Cybersecurity Plan has been revised, applicants must provide a brief explanation of the revisions. Applicants are not required to revise a Cybersecurity Plan that CISA has approved unless CISA notifies the applicant that the plan does not meet plan requirements.

Eligible applicants must coordinate with the appropriate Cybersecurity and CISA Regional Representatives before submitting their Cybersecurity Plan, Investment Justifications (IJ), and/or Project Worksheet (PW) (See [Section G](#) of this funding notice for relevant contact information). Additionally, all updated 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, please refer to [Appendices A-C](#).

CYBERSECURITY ACTIVITIES

The State Administrative Agency (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 2024 SLCGP requirements, Cybersecurity Plans must include the following activities:

- a. Conducting assessment and evaluations as the basis for individual projects throughout the life of the program; and
- b. Prioritizing key cybersecurity best practices and consulting [Cybersecurity Performance Goals \(CPGs\)](#).
 - i. The CPGs are a prioritized subset of information technology and operational technology cybersecurity practices aimed at meaningfully reducing risks to both critical infrastructure operations and the American people.
 - ii. 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.
 - iii. 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.
 - iv. 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, state, local, territorial (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 2024 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 2024 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 IJs.

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 D.11](#) in this funding notice.

MULTI-ENTITY PROJECTS

Multiple eligible entities (states or territories) can group together to address 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.

Multi-Entity Project Requirements and Process Overview

The following must be included in each of the participating state or territory group members' Cybersecurity Plans, the 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 2024 SLCGP for the projects in a multi-entity project is 20%.

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 2024 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.
- FEMA 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. Alignment to Program Purpose and the DHS and FEMA Strategic Plan

The FY 2024 SLCGP aligns with the National Cybersecurity Strategy by addressing three of the five pillars:

- Pillar One – Defend Critical Infrastructure;
- Pillar Two – Disrupt and Dismantle Threat Actors; and
- Pillar Four – Invest in a Resilient Future.

The FY 2024 SLCGP also addresses the [2020–2024 DHS Strategic Plan](#) by helping DHS achieve Goal 3: Secure Cyberspace and Critical Infrastructure. This includes Objective 3.2: Strengthen the Security and Resilience of Critical Infrastructure.

Additionally, the FY 2024 SLCGP supports the [2022–2026 FEMA Strategic Plan](#), which outlines a bold vision with three ambitious goals, including Goal 3: Promote

and Sustain a Ready FEMA and Prepared Nation, under which falls Objective 3.2: Posture FEMA to Meet Current and Emergent Threats.

The FY 2024 SLCGP also aligns with the [2023–2025 CISA Strategic Plan](#), which encompasses Goal 1: Cyber Defense, Goal 2: Risk Reduction and Resilience, and Goal 3: Operational Collaboration.

11. Performance Measures

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.

Performance Measures
Number of satisfactory annual tabletop and full-scale exercises to test Cybersecurity Plans.
Amount of grant funds budgeted for cybersecurity exercises.
Percentage of grant funds expended on exercise plans for entities.
Number of annual cyber risk assessments conducted to identify cyber risk management gaps and areas for improvement.
Number of employees that successfully completed phishing training.
Number of employees that attended and successfully completed awareness campaign training.
Number of employees that received role-based cybersecurity awareness training.
Number of employees that completed continuous learning activities on current cyber threats.
Number of employees that completed education or training on software security concepts. ¹
Number of supporting capabilities implemented to analyze network traffic and activities related to potential threats.
Number of multi-factor authentication (MFA) instances that were implemented for all remote access and privileged accounts.
Number of supporting programs created to anticipate and discontinue end-of-life software and hardware.
Number of known/fixed/default passwords and credentials prohibited for use on networks.
Number of unique sites that transitioned to a .gov internet domain.
Number of CISA-identified cybersecurity vulnerabilities that were addressed.
Number of Endpoint Detection Response Systems that were funded for implementation.
Number of capabilities ratings improved.
Number of funding improvements that were made for Continuity of Operations Plans.
Number of SAA performance metrics that were met.
Percent of increase in the use of CISA Services.
Numbers of instances of increased use of Data Encryption.
Numbers of instances of increased use of Enhanced Logging.
Numbers of systems adopting System Reconstitution.
Percentage of increase in the membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC).

B. Federal Award Information

1. Available Funding for the NOFO: \$279,873,562

¹ For the purpose of this grant, the term “software security concepts” refers to knowledge and understanding necessary to build secure software, including threat modeling, memory-safe languages, common classes of software defects, and adversarial thinking and training.

For FY 2024, 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 \$3,047,666 each, equaling 1% of total funds made available for the SLCGP in FY 2024. Each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) will receive a minimum of \$761,916, equaling 0.25% of the total funds made available for the SLCGP in FY 2024. \$59,173,633, 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 \$59,173,633, 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.

FY 2024 SLCGP Allocations

State/Territory	FY 2024 SLCGP Allocation	State/Territory	FY 2024 SLCGP Allocation
Alabama	\$5,825,678	Nevada	\$3,771,437
Alaska	\$3,399,745	New Hampshire	\$3,808,572
Arizona	\$5,032,682	New Jersey	\$5,184,599
Arkansas	\$4,778,475	New Mexico	\$3,893,800
California	\$11,845,702	New York	\$8,723,252
Colorado	\$4,791,605	North Carolina	\$8,037,374
Connecticut	\$4,122,302	North Dakota	\$3,454,693
Delaware	\$3,377,360	Ohio	\$7,598,799
District of Columbia	\$3,166,373	Oklahoma	\$5,005,631
Florida	\$8,620,815	Oregon	\$4,515,523
Georgia	\$7,456,494	Pennsylvania	\$8,015,678
Hawaii	\$3,469,262	Rhode Island	\$3,326,808
Idaho	\$3,899,009	South Carolina	\$5,454,484
Illinois	\$6,724,174	South Dakota	\$3,545,617
Indiana	\$5,987,571	Tennessee	\$6,368,577
Iowa	\$4,654,856	Texas	\$12,616,798
Kansas	\$4,288,916	Utah	\$3,947,782
Kentucky	\$5,489,622	Vermont	\$3,530,689
Louisiana	\$5,017,296	Virginia	\$6,446,009
Maine	\$4,038,646	Washington	\$5,546,984
Maryland	\$4,924,161	West Virginia	\$4,232,345
Massachusetts	\$4,816,189	Wisconsin	\$5,806,564
Michigan	\$7,178,365	Wyoming	\$3,345,507
Minnesota	\$5,474,363	Puerto Rico	\$3,830,330
Mississippi	\$4,975,106	U.S. Virgin Islands	\$780,956
Missouri	\$5,805,583	American Samoa	\$781,333

State/Territory	FY 2024 SLCGP Allocation	State/Territory	FY 2024 SLCGP Allocation
Montana	\$3,695,624	Guam	\$803,899
Nebraska	\$3,864,098	Northern Mariana Islands	\$779,450
Total		\$279,873,562	

2. **Projected Number of Awards:** 56
3. **Period of Performance:** 48 months

Extensions to the period of performance are allowed. For additional information on period of performance extensions, please refer to [Section H](#) of this NOFO.
4. **Projected Period of Performance Start Date:** 2/01/2025
5. **Projected Period of Performance End Date:** 1/31/2029
6. **Funding Instrument Type:** Grant

C. Eligibility Information

1. Eligible Applicants

a. States and U.S. Territories

2. Applicant Eligibility Criteria

All 56 states and territories, including any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands, are eligible to apply for SLCGP funds. The Governor-designated SLCGP SAA is the only entity eligible to submit SLCGP applications to DHS/FEMA. One or more states or territories may submit a multi-entity project.

“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.

3. Subawards and Beneficiaries

a. Subaward Allowability

Subawards are allowed for the SLCGP.

b. *Subrecipient Eligibility*

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 6 U.S.C. § 101(13)) defines a local government as:

- a. A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under state law), regional or interstate government entity, or agency or instrumentality of a local government;
- b. An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation²; and
- c. A rural community, unincorporated town or village, or other public entity.

c. *Other Subaward Information: 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.

The SAA for an SLCGP grant award is responsible for demonstrating the eligibility of each entity receiving assistance and should consult with FEMA if there is uncertainty regarding eligibility for a particular entity.

d. *Beneficiaries or Participants*

This NOFO and any subsequent federal awards create no rights or causes of action for any participant or beneficiary. There are no beneficiaries or other participants beyond recipients and subrecipients that benefit or participate in federal awards under this NOFO.

4. Other Eligibility Criteria/Restrictions

All applicants with a CISA-approved Cybersecurity Plan must submit their current Cybersecurity Plan to CISA via the FEMA SLCGP Inbox at FEMA-SLCGP@fema.dhs.gov no later than **January 30, 2025**, and annually thereafter on the same date throughout the

² Although tribes are not eligible to apply directly for SLCGP funding, they may be eligible subrecipients, and can receive SLCGP funding as a local government. Each individual SAA may determine whether and how much SLCGP funding to pass through to tribal entities. DHS does not have the authority to mandate that a certain percentage of SLCGP funds are directed to tribal governments.

grant's period of performance. Additional information on plan updates is described in Appendix C, "[Cybersecurity Plan](#)."

5. Cost Share or Match

Eligible entities must meet a 30% cost share requirement for the FY 2024 SLCGP. The cost share for multi-entity projects is 20%.

The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants must agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 30% of the total project costs (federal award amount plus cost share amount). For FY 2024, 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.

DHS/FEMA 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.

The cost share applies to each activity funded by the grant award rather than just to the cumulative total of all activities. Recipients must ensure that each activity's cost share is met. DHS interprets "activity" to mean each individual project under the submitted PW. A PW must include cost share for each project as well as Management and Administration (M&A). M&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.

a. *Types of Cost Share/Match*

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.

- i. Examples: State or local general fund monies.

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 program's goals, objectives, 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:

- i. **Example 1:** 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, 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.”
- ii. **Example 2:** 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 not be applicable. Instead, the hourly rate for an information technology specialist would be more reasonable and applicable.

Unrecovered Indirect Costs

With prior approval by FEMA, recipients may use unrecovered indirect costs for the cost share for FY 2024 SLCGP awards, as well as future 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. Recipients will be notified in writing if approval is granted. For additional information regarding indirect costs reference [Section D.13](#).

b. Cost Share Documentation

The source documentation for the cost share should be:

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.
2. Signed and dated by the donating company, person, etc.
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.

c. Calculating Cost Share for the Application

Applicants must make available non-federal funds or soft match (in-kind contributions) to carry out an SLCGP award in an amount not less than 30% of the total project costs (federal

award amount plus cost share amount). The cost share for the multi-entity projects is 20% for FY 2024.

Formula: Federal Award Amount / Federal Share Percentage = Total Project Cost
Total Project Cost x Cost Share Percentage = Cost Share Amount

- i. **Example:** If the federal award is \$1,000,000 with a 70% federal share percentage and a 30% cost share percentage, the cost share amount is calculated below:
 - \$1,000,000 (Federal Award Amount) / .70 = \$1,428,571 (Total Project Cost)
 - \$1,428,571 x .30 = \$428,571.30 (Cost Share Amount)

d. Calculating Cost Share for Projects

Cost share must be provided on a project basis. To calculate cost share for a project, please see the following formula and example:

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

- i. **Example:** If the total project cost is \$125,000, the cost share percentage of the project is 30% and the federal percentage share of the project is 70%, the cost share amount for the project and federal amount for the project is calculated below:
 - \$125,000 x .30 = \$37,500 (Cost Share Amount for Project)
 - \$125,000 x .70 = \$87,500 (Federal Share Amount for Project)

e. Future Cost Share Amounts

For SLCGP planning purposes, the following chart indicates the federal share and cost share percentages for SLCGP FY 2022 - 2025:

Federal fiscal year (FFY)	Single Entity Project		Multi-Entity Project	
	Federal share percentage	Non-federal cost share percentage	Federal share percentage	Non-federal cost share percentage
2022	90%	10%	100%	0%
2023	80%	20%	90%	10%
2024	70%	30%	80%	20%
2025	60%	40%	70%	30%

f. Cost Share Waiver

The Secretary of Homeland Security (or designee) may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. The Homeland Security Act of 2002, as amended, requires SLCGP recipients in FY 2024 to provide a non-federal cost share of 30% if they are applying as a single entity (6 U.S.C. § 665g(m)(1)). However, DHS is not able to provide additional funds even if it does grant a cost share waiver. The federal funding will remain at the same amount as indicated by the statutory formula.

Additionally, in accordance with 48 U.S.C. § 1469a cost share requirements 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 are waived.

Economic Hardship Factors

6 U.S.C. § 665g(m)(2)(C) requires the Secretary of Homeland Security (or designee) to consider the following factors when determining economic hardship:

- a. Changes in rates of unemployment in the jurisdiction from previous years;
- b. Changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. § 2011 et seq.) from previous years; and
- c. Any other factors the Secretary considers appropriate.

For FY 2024, the Secretary (or designee) will consider the following additional factors in determining economic hardship:

- a. Demonstration that the rate of unemployment has exceeded the annual national average rate of unemployment for three of the past five years;
- b. Demonstration that the entity has filed for bankruptcy or been placed under third-party financial oversight or receivership within the past three years; and
- c. For local units of government only, demonstration that those localities have areas within them that are designated as “disadvantaged” on the Climate and Economic Justice Screening Tool (CEJST).

To be considered for a cost share waiver, eligible entities must meet at least one of the five factors described above, but do not necessarily need to meet all of them. Requests for waivers will be considered on a case-by-case basis and evaluated holistically. The applicant is required to submit documentation supporting their request for an Economic Hardship Waiver at the award level at time of the application by attaching the supporting document to the grant application.

Cost Share Waiver Request Requirements

To request a waiver, an eligible entity must submit a written narrative, including the following three categories to demonstrate economic hardship, with its FY 2024 SLCGP application submission in FEMA GO:

- a. History: A description of the entity’s background/history of economic hardship.
- b. Austerity: Describe any measures the entity has taken to address economic hardship.
- c. Operational Impact: Describe how the lack of a waiver will impact the entity’s ability to develop, implement, or revise a Cybersecurity Plan or address imminent cybersecurity threats.

A detailed justification explaining why the state (or specific local government(s) or specific project(s) if requesting only a partial waiver) is unable to fulfill the cost share requirement. The applicant must identify specific economic hardship(s) and address the factors listed above.

Approval Process

Once a decision on a waiver request is made, the SLCGP SAA will be notified in writing. If approved, the award package will indicate that the cost share has been waived in full or in part and might indicate a requirement for the state to submit a revised budget and/or scope (as applicable) for the identified project(s). If the waiver request is approved after the award has been issued, FEMA will amend the award package to indicate that the cost share has been waived in full or in part and whether the recipient must submit a revised budget and/or scope (as applicable) for the identified project(s).

Questions regarding the cost share waiver process may be directed to your FEMA Preparedness Officer by emailing FEMA-SLCGP@fema.dhs.gov.

D. Application and Submission Information

1. Key Dates and Times

- a. *Application Start Date:* 09/23/2024 at 9:00 AM ET
- b. *Application Submission Deadline:* 12/3/2024 at 5:00 PM ET

All applications **must** be received by the established deadline.

[FEMA's Grants Outcomes System](#) (FEMA GO) automatically records proof of timely submission and the system generates an electronic date/time stamp when FEMA GO successfully receives the application. The individual with the Authorized Organization Representative role that submitted the application will also receive the official date/time stamp and a FEMA GO tracking number in an email serving as proof of their timely submission. For additional information on how an applicant will be notified of application receipt, see the subsection titled "[Timely Receipt Requirements and Proof of Timely Submission](#)" in [Section D](#) of this NOFO.

FEMA will not review applications that are received after the deadline or consider these late applications for funding. FEMA may, however, extend the application deadline on request for any applicant who can demonstrate that good cause exists to justify extending the deadline. Good cause for an extension may include technical problems outside of the applicant's control that prevent submission of the application by the deadline, other exigent or emergency circumstances, or statutory requirements for FEMA to make an award.

Applicants experiencing technical problems outside of their control must notify FEMA as soon as possible and before the application deadline. Failure to timely notify FEMA of the issue that prevented the timely filing of the application may preclude consideration of the award. "Timely notification" of FEMA means the following: prior to the application deadline and within 48 hours after the applicant became aware of the issue.

A list of FEMA contacts can be found in [Section G](#) of this NOFO, "[DHS Awarding Agency Contact Information](#)." For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET. For programmatic or grants management questions, please contact

your Preparedness Officer or Grants Management Specialist. If applicants do not know who to contact or if there are programmatic questions or concerns, please contact FEMA Grants News at fema-grants-news@fema.dhs.gov, Monday through Friday, 9:00 AM – 5:00 PM ET.

c. ***Anticipated Award Date:*** No later than 02/01/2024

d. ***Other Key Dates***

Event	Suggested Deadline for Completion
Obtaining Unique Entity Identifier (UEI) number	Four weeks before actual submission deadline
Obtaining a valid Employer Identification Number (EIN)	Four weeks before actual submission deadline
Creating an account with login.gov	Four weeks before actual submission deadline
Registering in SAM or updating SAM registration	Four weeks before actual submission deadline
Registering Organization in FEMA GO	Prior to beginning application
Submitting complete application in FEMA GO	One week before actual submission deadline

2. **Agreeing to Terms and Conditions of the Award**

By submitting an application, applicants agree to comply with the requirements of this NOFO and the terms and conditions of the award, should they receive an award.

3. **Address to Request Application Package**

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

Hard copies of the NOFO can be downloaded at [Grants.gov](https://www.fema.gov/grants) or obtained via email from the Awarding Office points of contact listed in Section G of this NOFO, “[DHS Awarding Agency Contact Information](#)” or by TTY (800) 462-7585.

4. **Requirements: Obtain a Unique Entity Identifier (UEI) and Register in the System for Award Management ([SAM.gov](https://sam.gov))**

Each applicant, unless they have a valid exception under 2 C.F.R. §25.110, must:

- a. Be registered in SAM.gov before application submission.
- b. Provide a valid UEI in its application.
- c. Continue to always maintain an active SAM registration with current information during the federal award process. Note: Per 2 C.F.R. § 25.300, subrecipients are NOT required to go through the full SAM registration process. First-tier subrecipients (meaning entities receiving funds directly from the recipient) are only required to obtain a UEI through SAM, but they are not required to complete the full SAM registration in order to obtain a UEI. Recipients may not make subawards unless the subrecipient has obtained and provided the UEI.

Lower-tier subrecipients (meaning entities receiving funds passed through by a higher-tier subrecipient) are not required to have a UEI and are not required to register in SAM. Applicants are also not permitted to require subrecipients to complete a full registration in SAM beyond obtaining the UEI.

5. Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application

Applying for an award under this program is a multi-step process and requires time to complete. Applicants are encouraged to register early as the registration process can take four weeks or more to complete. Therefore, registration should be done in sufficient time to ensure it does not impact your ability to meet required submission deadlines.

Please review the table above for estimated deadlines to complete each of the steps listed. Failure of an applicant to comply with any of the required steps before the deadline for submitting an application may disqualify that application from funding.

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

- a. Apply for, update, or verify their UEI number and Employer Identification Number (EIN) from the Internal Revenue Service;
- b. In the application, provide an UEI number;
- c. Have an account with login.gov;
- d. Register for, update, or verify their 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 <https://www.fema.gov/grants/guidance-tools/fema-go/startup>
- f. Submit the complete application in FEMA GO; 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.

Applicants are advised that FEMA may not make a federal award until the applicant has complied with all applicable SAM requirements. Therefore, an applicant's SAM registration must be active not only at the time of application, but also during the application review period and when FEMA is ready to make a federal award. Further, as noted above, an applicant's or recipient's SAM registration must remain active for the duration of an active federal award. If an applicant's SAM registration is expired at the time of application, expires during application review, or expires any other time before award, FEMA may determine that the applicant is not qualified to receive a federal award and use that determination as a basis for making a federal award to another applicant.

Per 2 C.F.R. § 25.110I(2)(iii), 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 by contacting FEMA Grants News at fema-grants-news@fema.dhs.gov and providing the details of the circumstances that prevent completion of these requirements. If FEMA determines that there are exigent circumstances and FEMA has decided to make an award, the applicant will be required to obtain an UEI number, if applicable, and complete SAM registration within 30 days of the federal award date.

6. Electronic Delivery

DHS is participating in the Grants.gov initiative to provide the grant community with a single site to find and apply for grant funding opportunities. DHS encourages or requires applicants to submit their applications online through Grants.gov, depending on the funding opportunity.

For this funding opportunity, FEMA requires applicants to submit applications through FEMA GO.

7. How to Register to Apply

a. General Instructions:

Registering and applying for an award under this program is a multi-step process and requires time to complete. Read the instructions below about registering to apply for FEMA funds. Applicants should read the registration instructions carefully and prepare the information requested before beginning the registration process. Reviewing and assembling the required information before beginning the registration 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 an UEI number, an EIN, an active SAM registration and an active SAM registration to apply for a federal award under this funding opportunity.

b. Obtain an 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).

c. Obtain Employer Identification Number

All entities applying for funding must provide an Employer Identification Number (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>.

d. 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 here:

https://secure.login.gov/sign_up/enter_email?request_id=34f19fa8-14a2-438c-8323-a62b99571fd3.

Applicants only have to create a login.gov account once. For applicants that are existing SAM users, use the same email address for the login.gov account as with 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>.

e. Register with SAM:

All applicants applying online through FEMA GO must register with SAM. Failure to register with SAM will prevent an applicant from completing the application in FEMA GO. SAM registration must be renewed annually. Organizations will be issued a UEI number with the completed SAM registration.

For more detailed instructions for registering with SAM, refer to

<https://apply07.grants.gov/help/html/help/Register/RegisterWithSAM.htm>

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 last three years, if applicable.

I. ADDITIONAL SAM REMINDERS

Existing SAM.gov account holders should check their account to make sure it is "ACTIVE." SAM registration should be completed at the very beginning of the application period and should be renewed annually to avoid being "INACTIVE." **Please allow plenty of time before the grant application submission deadline to obtain an UEI number and then to register in SAM. It may be four weeks or more after an applicant submits the SAM registration before the registration is active in SAM, and then it may be an additional 24 hours before FEMA's system recognizes the information.**

It is imperative that the information applicants provide is correct and current. Please ensure that your organization's name, address, and EIN are up to date in SAM and that the UEI number used in SAM is the same one used to apply for all other FEMA awards. Payment under any FEMA award is contingent on the recipient's having a current SAM registration.

II. HELP WITH SAM

The SAM quick start guide for new recipient registration and SAM video tutorial for new applicants are tools created by the General Services Administration

(GSA) to assist those registering with SAM. If applicants have questions or concerns about a SAM registration, please contact the Federal Support Desk at <https://www.fsd.gov/fsd-gov/home.do> or call toll free (866) 606-8220f.

f. 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 <https://www.fema.gov/grants/guidance-tools/fema-go/startup>

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

- Google Chrome
- Mozilla Firefox
- Apple Safari
- Microsoft Edge

Users who attempt to use tablet type devices or other browsers may encounter issues with using FEMA GO.

8. Submitting the Application

Applicants will be prompted to submit the standard application information and any program-specific information required as described in Section D.10 of this NOFO, "[Content and Form of Application Submission](#)." The Standard Forms (SF) may be accessed in the Forms tab under the <https://grants.gov/forms/forms-repository/sf-424-family> Applicants should review these forms before applying to ensure they have all the information required.

After submitting the final application, FEMA GO will provide either an error message or a successfully received transmission in the form of an email sent to the AOR that submitted the application. Applicants using slow internet connections, such as dial-up connections, should be aware that transmission can take some time before FEMA GO receives your application.

For additional application submission requirements, including program-specific requirements, please refer to the subsection titled "Content and Form of Application Submission" under Section D of this NOFO.

9. Timely Receipt Requirements and Proof of Timely Submission

All applications must be completed in FEMA GO by the application deadline. FEMA GO automatically records proof of timely submission and the system generates an electronic date/time stamp when FEMA GO successfully receives the application. The individual with the AOR role that submitted the application will also receive the official date/time stamp and a FEMA GO tracking number in an email serving as proof of their timely submission on the date and time that FEMA GO received the application.

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

10. Content and Form of Application Submission

a. *Standard Required Application Forms and Information*

The following forms or information are required to be submitted via FEMA GO. The Standard Forms (SF) are also available at <https://grants.gov/forms/forms-repository/sf-424-family>

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

b. *Program-Specific Required Forms and Information*

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

INVESTMENT JUSTIFICATION (IJ) 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 which 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 more than four IJs can be submitted with the application.

- **Objective:** Each submitted IJ corresponds 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.”

INVESTMENT JUSTIFICATION IMPLEMENTATION SCHEDULE

The implementation schedule table should be used as a planning tool for the key activities and milestones associated with each project identified in the Cybersecurity Plan. Applicants must also describe how implementing the plan will be measured (metrics). For each project and each year of the grant, the applicant should include the activities necessary to accomplish the goals of each project, as well as the estimated start and completion dates (by calendar quarter) for each activity. The standard definition of a project is a temporary endeavor with a defined beginning and end (usually time-constrained, and often constrained by funding or a deliverable), undertaken to meet unique goals and objectives, typically to bring about beneficial change or added value. Applying this standard to projects using preparedness grant funds, a project is a related set of activities and purchases supporting the building or sustaining of core capabilities; and is associated with a single entity responsible for execution.

Download IJ Template from FEMA’s website or access the IJ Template on [Grants.gov](https://www.fema.gov/grants). 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

Download the PW from FEMA’s website or access the PW on [Grants.gov](https://www.fema.gov/grants). 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, Management and Administration (M&A) costs, amount and source of cost share, etc. The Planning, Organization, Equipment, Training, and/or Exercises (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.

The PW template provides drop-down selections for several of the project attributes. All project attribute fields must be completed for the PW to be considered complete. Incomplete PWs will not be accepted. 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 can email questions about the IJ, PW or application requirements to FEMA-SLCGP@fema.dhs.gov. User guides are available for SLCGP IJs and PWs on the [SLCGP website](#).

11. Other Submission Requirements

Refer to 2 C.F.R.200 for any additional submission requirements.

12. Intergovernmental Review

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 (See <https://www.archives.gov/federal-register/codification/executive-order/12372.html>; [Intergovernmental Review \(SPOC List\) \(whitehouse.gov\)](#)).

13. Funding Restrictions and Allowable Costs

All costs charged to federal awards (including both federal funding and any non-federal matching or cost sharing funds) must comply with applicable statutes, rules and regulations, and policies, this NOFO, and the terms and conditions of the federal award. They must also comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200 unless otherwise indicated in the NOFO or 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). The following identifies a list of activities for which a recipient may not use federal funds and any cost sharing or matching funds under federal awards:

- Matching or cost sharing requirements for other federal grants and cooperative agreements (see 2 C.F.R. § 200.306).
- Lobbying or other prohibited activities under 18 U.S.C. § 1913 or 2 C.F.R. § 200.450.
- Prosecuting claims against the federal government or any other government entity (see 2 C.F.R. § 200.435) See subsections below for information on any other funding restrictions.

Please see Appendix D, “[POETE Solution Areas for Investments](#)” for details on other allowable costs.

Unallowable Costs

For FY 2024 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. To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building.);
 - 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 has previously used SLT funds to support the same or similar uses; and
 - j. For any recipient or subrecipient cost-sharing contribution.
- a. ***Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services***

Recipients, subrecipients, and their contractors must comply with the prohibitions set forth in Section 889 of the [John S. McCain National Defense Authorization Act](#) for Fiscal Year 2019, Pub. L. No. 115-232 (2018) (FY 2019 NDAA) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. The FY 2019 NDAA and these regulations, as they apply to recipients, subrecipients, and their contractors and subcontractors, provide for two distinct prohibitions: (1) prevent the use of federal award funds to procure or obtain covered telecommunications equipment or services; and (2) prevent the use of federal award funds to contract with an entity that uses such covered telecommunications equipment or services. Guidance is available at [FEMA Policy #405-143-1 - Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services](#)

Additional guidance is available at [Contract Provisions Guide: Navigating Appendix II to Part 2-0 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards \(fema.gov\)](#).

FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

- Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;

- Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or
- Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

I. REPLACEMENT EQUIPMENT AND SERVICES

FEMA grant funding may be permitted to procure replacement equipment and services covered by this prohibition, provided the costs are otherwise consistent with the requirements of the NOFO.

II. DEFINITIONS

Per section 889(f)(2)-(3) of the FY 2019 NDAA and 2 C.F.R. § 200.216, covered telecommunications equipment or services means:

- Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);
- For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- Telecommunications or video surveillance services provided by such entities or using such equipment; or
- Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the People's Republic of China.

Examples of the types of products covered by this prohibition include phones, internet, video surveillance, and cloud servers when produced, provided, or used by the entities listed in the definition of “covered telecommunications equipment or services.” See 2 C.F.R. § 200.471b.

b. Pre-Award Costs

Pre-award costs are allowable only with the prior written approval of DHS/FEMA 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 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 FEMA that the expenses have been reviewed and that FEMA 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.

FEMA 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. See Section H of this NOFO for general procurement under grants requirements.

c. *Management and Administration (M&A) Costs*

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

Subrecipients may also retain a maximum of up to 5% of the 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, 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. Characteristics of M&A expenses can include the following:

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

d. *Indirect Facilities & Administrative (F&A) Costs*

Indirect (F&A) costs (IDC) mean those costs incurred for a common or joint purpose benefitting more than one cost objective and not readily assignable to the cost

objectives specifically benefitted, without effort disproportionate to the results achieved. IDC are allowable by the recipient [and subrecipients] as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. 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 who do not have a current negotiated IDC rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to FEMA for further instructions. Applicants who wish to use a cost allocation plan in lieu of an IDC rate proposal must reach out to the FEMA Point of Contact 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.

Establishing Indirect Cost Rates

The processes for establishing the indirect cost rate varies 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(a)(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 state or local governmental entity, indirect cost rate procedures are established in 2 C.F.R. 200, Appendix VII. Per Paragraph D.1.b. of Appendix VII, state or local governmental entities receiving grant funds must develop an indirect cost rate proposal.
3. If the state or local entity receives more than \$35 million in grant funding in a fiscal year, the proposal must be approved by the cognizant agency.
4. If a state or local entity 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.
5. If a state or local governmental 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)).

Applicants should reach out to their Grants Management Specialist for further instructions.

e. *Evaluation Costs*

Evaluation costs are allowable. See Section H.2 “Program Evaluation” for more details.

f. *Other Direct Costs*

Funding guidelines established within this section support the development, updating, and implementing a Cybersecurity Plan. Allowable investments made in support of this goal must fall into POETE, aligned to closing capability gaps or sustaining

capabilities. More information on the POETE solution areas can be found in Appendix D, “[POETE Solution Areas for Investments](#).”

E. Application Review Information

1. Application Evaluation Criteria

a. *Programmatic Criteria*

DHS/FEMA will evaluate the FY 2024 SLCGP applications for completeness and applicant eligibility. DHS/CISA will evaluate the FY 2024 SLCGP applications for adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments.

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

- a. Eligible entities understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments;
- b. Eligible entities implement security protections commensurate with risk; and
- c. Eligible entities ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

In addition to the above, DHS/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.

b. *Financial Integrity Criteria*

Prior to making a federal award, FEMA is required by 31 U.S.C. § 3354, as enacted by the Payment Integrity Information Act of 2019, Pub. L. No. 116-117 (2020); 41 U.S.C. § 2313; and 2 C.F.R. § 200.206 to review information available through any Office of Management and Budget (OMB)-designated repositories of government wide eligibility qualification or financial integrity information, including whether SAM.gov identifies the applicant as being excluded from receiving federal awards or is flagged for any integrity record submission. FEMA may also pose additional questions to the applicant to aid in conducting the pre-award risk review. Therefore, application evaluation criteria may include the following risk-based considerations of the applicant:

- i. Financial stability;
- ii. Quality of management systems and ability to meet management standards;
- iii. History of performance in managing federal award;
- iv. Reports and findings from audits; and
- v. Ability to effectively implement statutory, regulatory, or other requirements.

c. *Supplemental Financial Integrity Criteria and Review*

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently \$250,000:

- i. FEMA is required by 41 U.S.C. § 2313 and 2 C.F.R. § 200.206(a)(2) to review and consider any information about the applicant, including information on the applicant's immediate and highest-level owner, subsidiaries, and predecessors, if applicable, that is in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the [Federal Awardee Performance and Integrity Information System](#) (FAPIIS).
- ii. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.
- iii. FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.206.

2. Review and Selection Process

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.

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 IJs and PWs. FEMA will use a checklist to verify compliance with all administrative and eligibility criteria identified in the NOFO.

Applicants must demonstrate how investments support closing capability gaps or sustaining capabilities. CISA will review IJs and PWs 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 SAFECOM Guidance (see Section F.3.d below). 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.

F. Federal Award Administration Information

1. Notice of Award

2. 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, please see Section C.3.b. of this NOFO.

a. Documenting the Pass-Through

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

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

b. 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.

c. *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 to FEMA. Once the proposed costs and activities are reviewed by FEMA and CISA, the recipient will be notified, and the funding will be released.

d. *Timing*

After the funds have been released, FY 2024 SLCGP recipients must submit a letter to FEMA 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 FEMA-SLCGP@fema.dhs.gov. FEMA will send a copy of the letter to CISA.

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) Pass-Through Deadline Date	Letter Submission from SAA to FEMA Due Date
Project A	April 15, 2024	May 30, 2024	NLT June 9, 2024
Project B	May 15, 2024	June 29, 2024	NLT July 9, 2024
Project C	June 15, 2024	July 30, 2024	NLT August 9, 2024

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

As stated in the previous section, the signatory authority of the SLCGP recipient entity must certify in writing to FEMA 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.

3. Administrative and National Policy Requirements

4. Reporting

Recipients are required to submit various financial and programmatic reports as a condition of award acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

a. Financial Reporting Requirements

I. FEDERAL FINANCIAL REPORT (FFR)

Recipients must report obligations and expenditures through the FFR form (SF-425) to FEMA.

Recipients may review the Federal Financial Reporting Form (FFR) (SF-425) at <https://apply07.grants.gov/apply/forms/sample/SF425-V1.0.pdf>

Recipients must file the FFR electronically using FEMA GO.

II. FFR REPORTING PERIODS AND DUE DATES

An FFR must be submitted quarterly throughout the POP, including partial calendar quarters, as well as in periods where no grant award activity occurs. The final FFR is due within 120 calendar days after the end of the POP. Future awards and fund drawdowns may be withheld if these reports are delinquent, demonstrate lack of progress, or are insufficient in detail.

Except for the final FFR due at 120 days after the end of the POP for purposes of closeout, the following reporting periods and due dates apply for the FFR:

Reporting Period	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

b. Programmatic Performance Reporting Requirements

I. PERFORMANCE AND PROGRESS REPORTING

Recipients are responsible for providing updated performance reports on an annual basis, consistent with section 2200A(q)(1) of the Homeland Security Act of 2002, as an attachment in FEMA GO. The annual PPR submission is due Jan. 30 of each year to account for the previous calendar year.

This reporting will include a:

- Brief narrative of overall project(s) status;
- Summary of project expenditures;
- Description of any potential issues that may affect project completion;
- Data collected for DHS performance measures; and
- The report must be signed by the Authorized Official or Signatory Authority.

Questions regarding programmatic performance reporting should be submitted to the recipient's assigned FEMA Preparedness Officer by emailing the SLCGP general email inbox at FEMA-SLCGP@fema.dhs.gov. Please include the recipient's grant award number with the email.

Additionally, any questions regarding financial reporting should be directed to your Grants Management Specialist by contacting ASK-GMD@fema.dhs.gov.

c. Closeout Reporting Requirements

I. CLOSEOUT REPORTING

Within 120 calendar days after the end of the period of performance for the prime award or after an amendment has been issued to close out an award before the original POP ends, recipients must liquidate all financial obligations and must submit the following:

- i. The final request for payment, if applicable.
- ii. The final FFR (SF-425).

- iii. The final progress report detailing all accomplishments, including a narrative summary of the impact of those accomplishments throughout the period of performance. If applicable, the recipient must include with the final progress report an inventory of all construction projects.
- v. Other documents required by this NOFO, terms and conditions of the award, or other FEMA guidance. If the final FFR and performance report periods coincide with the end of the period of performance, FEMA has discretion under 2 C.F.R. Part 200 to waive the last quarterly/semiannual/annual reports and only require the final FFR and performance report for closeout purposes. 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(d).

In addition, pass-through entities are responsible for closing out their subawards as described in 2 C.F.R. § 200.344; subrecipients are still required to submit closeout materials within 90 calendar days of the period of performance end date. When a subrecipient completes all closeout requirements, pass-through entities must promptly complete all closeout actions for subawards in time for the recipient to submit all necessary documentation and information to FEMA during the closeout of the prime award.

After the prime award closeout reports have been reviewed and approved by FEMA, a closeout notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be de-obligated, and address the requirement of maintaining the grant records for at least three years from the date of the final FFR. The record retention period may be longer, such as due to an audit or litigation, for equipment or real property used beyond the period of performance, or due to other circumstances outlined in 2 C.F.R. § 200.334.

The recipient is responsible for refunding to FEMA any balances of unobligated cash that FEMA paid that are not authorized to be retained per 2 C.F.R. § 200.344(d).

II. ADMINISTRATIVE CLOSEOUT

Administrative closeout is a mechanism for FEMA to unilaterally move forward with closeout of an award using available award information in lieu of final reports from the recipient per 2 C.F.R. § 200.344(h)-(i). It is a last resort available to FEMA, and if FEMA needs to administratively close an award, this may negatively impact a recipient's ability to obtain future funding. This mechanism can also require FEMA to make cash or cost adjustments and ineligible cost determinations based on the information it has, which may result in identifying a debt owed to FEMA by the recipient.

When a recipient is not responsive to FEMA's reasonable efforts to collect required reports needed to complete the standard closeout process, FEMA is required under 2 C.F.R. § 200.344(h) to start the administrative closeout process within the regulatory timeframe. FEMA will make at least three written attempts to collect required reports

before initiating administrative closeout. If the recipient does not submit all required reports in accordance with 2 C.F.R. § 200.344, this NOFO, and the terms and conditions of the award, FEMA must proceed to administratively close the award with the information available within one year of the period of performance end date. Additionally, if the recipient does not submit all required reports within one year of the period of performance end date, per 2 C.F.R. § 200.344(i), FEMA must report in Contracting Performance Assessment Reporting System (CPARS) the recipient's material failure to comply with the terms and conditions of the award.

If FEMA administratively closes an award where no final FFR has been submitted, FEMA uses that administrative closeout date in lieu of the final FFR submission date as the start of the record retention period under 2 C.F.R. § 200.334.

In addition, if an award is administratively closed, FEMA may decide to impose remedies for noncompliance per 2 C.F.R. § 200.339, consider this information in reviewing future award applications, or apply special conditions to existing or future awards.

d. *Additional Reporting Requirements*

I. DISCLOSING INFORMATION PER 2 C.F.R. § 180.335

This reporting requirement pertains to disclosing information related to government-wide suspension and debarment requirements. Before a recipient enters into a grant award with FEMA, the recipient must notify FEMA if it knows if it or any of the recipient's principals under the award fall under one or more of the four criteria listed at 2 C.F.R. § 180.335:

- i. Are presently excluded or disqualified;
- ii. Have been convicted within the preceding three years of any of the offenses listed in 2 C.F.R. § 180.800(a) or had a civil judgment rendered against it or any of the recipient's principals for one of those offenses within that time period;
- iii. Are presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state or local) with commission of any of the offenses listed in 2 C.F.R. § 180.800(a); or
- iv. Have had one or more public transactions (federal, state, or local) terminated within the preceding three years for cause or default.

At any time after accepting the award, if the recipient learns that it or any of its principals falls under one or more of the criteria listed at 2 C.F.R. § 180.335, the recipient must provide immediate written notice to FEMA in accordance with 2 C.F.R. § 180.350.

II. REPORTING OF MATTERS RELATED TO RECIPIENT INTEGRITY AND PERFORMANCE

Appendix XII to 2 C.F.R. Part 200 sets forth a term and condition related to recipient integrity and performance matters that will apply to all federal awards under this funding opportunity. If the total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies exceeds \$10,000,000 for any period of time during the period of performance of a federal

award under this funding opportunity, then a recipient must maintain the currency of information reported in the Contracting Performance Assessment Reporting System (CPARS) about civil, criminal, or administrative proceedings described in paragraph 2 of Appendix XII at the reporting frequency described in paragraph 4 of Appendix XII.

III. SINGLE AUDIT REPORT

A recipient that expends \$750,000 or more during the recipient's fiscal year in federal awards (as defined by 2 C.F.R. § 200.1) must have a single audit conducted in accordance with 2 C.F.R. § 200.514 except when it elects to have a program-specific audit conducted in accordance with 2 C.F.R. § 200.501. The audit must be conducted in accordance with 2 C.F.R. Part 200, Subpart F and, as required by 2 C.F.R. § 200.514, in accordance with the U.S. Government Accountability Office (GAO) Generally Accepted Government Auditing Standards, which can be found on the Yellow Book page of the GAO website.

5. Monitoring and Oversight

The regulation at 2 C.F.R. § 200.337 provides DHS and any of its authorized representatives with the right of access to any documents, papers, or other records of the recipient (and any subrecipients) that are pertinent to a federal award in order to make audits, examinations, excerpts, and transcripts. 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. Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review project accomplishments and management control systems to evaluate project accomplishments and to provide any required technical assistance. During site visits, DHS may review a recipient's or subrecipient's files pertinent to the federal award and interview and/or discuss these files with the recipient's or subrecipient's personnel. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

Effective monitoring and oversight help FEMA and CISA ensure that recipients use grant funds for their intended purpose(s); verify that projects undertaken are consistent with approved plans; and ensure that recipients make adequate progress toward stated goals and objectives. Additionally, monitoring serves as the primary mechanism to ensure that recipients comply with applicable laws, rules, regulations, program guidance, and requirements. FEMA and CISA regularly monitor all grant programs both financially and programmatically in accordance with federal laws, regulations (including 2 C.F.R. Part 200), program guidance, and the terms and conditions of the award. All monitoring efforts ultimately serve to evaluate progress towards grant goals and proactively target and address issues that may threaten grant success during the period of performance.

FEMA and CISA staff will periodically monitor recipients to ensure that administrative processes, policies and procedures, budgets, and other related award criteria are meeting Federal Government-wide and FEMA regulations. Aside from reviewing quarterly financial and programmatic reports, FEMA and CISA may also conduct enhanced monitoring through either desk-based reviews, onsite monitoring visits, or both. Enhanced monitoring will

involve the review and analysis of the financial compliance and administrative processes, policies, activities, and other attributes of each federal assistance award, and it will identify areas where the recipient may need technical assistance, corrective actions, or other support.

Financial and programmatic monitoring are complementary processes within the overarching monitoring strategy that function together to ensure effective grants management, accountability, and transparency; validate progress against grant and program goals; and safeguard federal funds against fraud, waste, and abuse. Financial monitoring primarily focuses on statutory and regulatory compliance with administrative grant requirements, while programmatic monitoring seeks to validate and assist in grant progress, targeting issues that may be hindering achievement of project goals and ensuring compliance with the purpose of the grant and grant program. Both monitoring processes are similar in that they feature initial reviews of all open awards, and additional, in-depth monitoring of grants requiring additional attention.

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: 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.

Financial and Program Monitoring Overview and Approach

CISA and FEMA's approach to financial and program monitoring provides a standard monitoring framework that promotes consistent processes across all monitoring staff. There are four core components of the monitoring process:

1. **Monitoring Assessment:** Monitoring staff measure each grant's monitoring needs using a system of pre-determined evaluation criteria. The criteria help assess the recipient and potential challenges to the success of the grant award.
2. **Monitoring Selection and Scheduling:** Monitoring staff make selection and scheduling decisions in accordance with applicable statutory requirements, such as the Homeland Security Act of 2002, as amended, and consider the results of the monitoring assessment process.
3. **Monitoring Activities:** Financial monitoring activities include cash analysis, desk reviews, and site visits. Grants Management Specialists are responsible for conducting quarterly or semi-annual reviews of all grants via cash analysis. Program monitoring is conducted by FEMA and CISA and will include a review of the grant program performance, particularly the implementation of the recipient's project activities toward

meeting the goals and objectives in the approved Cybersecurity Plan. Desk reviews and site visits are additional monitoring activities conducted on grants where the monitoring assessment process identified the need for additional monitoring and validated the use of CISA and FEMA resources for these activities.

4. **Post-Monitoring Actions:** Monitoring staff may follow up with recipients via post-monitoring actions based on the outcomes of monitoring activities. Post monitoring actions include conducting additional monitoring, reviewing Corrective Action Plans (CAP), and monitoring the progress of CAP deliverables, documenting the resolution of identified corrective actions and issues, providing technical assistance and recipient training, and debt collection.

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information

a. *FEMA Program Office Contact*

The FEMA SLCGP Program Office can provide general information on all FEMA grant programs and additional guidance surrounding questions on SLCGP administration. If desired, applicants and recipients may contact their FEMA Preparedness Officer, the Team Lead, or the Cyber Branch Chief for more information by email at FEMA-SLCGP@fema.dhs.gov.

b. *CISA Grant Program Office Contact*

The CISA Grant Program Office has programmatic staff as well as regional staff 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/or regional staff for more information by email at SLCGPinfo@cisa.dhs.gov.

c. *FEMA Grants News*

FEMA Grants News is a non-emergency comprehensive management and information resource developed by FEMA for grants stakeholders. 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. When necessary, recipients will be directed to a federal point of contact who can answer specific programmatic questions or concerns. FEMA Grants News can be reached by e-mail at fema-grants-news@fema.dhs.gov OR by phone at (800) 368-6498, Monday through Friday, 9:00 AM – 5:00 PM ET.

d. *Grant Programs Directorate (GPD) Award Administration Division*

GPD's Award Administration Division (AAD) provides support regarding financial matters and budgetary technical assistance. Additional guidance and information can be obtained by contacting the AAD's Help Desk via e-mail at ASK-GMD@fema.dhs.gov.

e. *Equal Rights*

The FEMA Office of Civil Rights (OCR) is responsible for compliance with and enforcement of federal civil rights obligations in connection with programs and

services conducted by FEMA and recipients of FEMA financial assistance. All inquiries and communications about federal civil rights compliance for FEMA grants under this NOFO should be sent to FEMA-CivilRightsOffice@fema.dhs.gov.

f. *Environmental Planning and Historic Preservation*

GPD's EHP Team provides guidance and information about the EHP review process to recipients and subrecipients. All inquiries and communications about GPD projects under this NOFO or the EHP review process, including the submittal of EHP review materials, should be sent to gpdehpinfo@fema.dhs.gov.

2. Systems Information

a. *FEMA GO*

For technical assistance with the FEMA GO system, please contact the FEMA GO Helpdesk at femago@fema.dhs.gov or (877) 585-3242, Monday through Friday, 9:00 AM – 6:00 PM ET.

H. Additional Information

1. Termination Provisions

FEMA may terminate a federal award in whole or in part for one of the following reasons. FEMA and the recipient must still comply with closeout requirements at 2 C.F.R. §§ 200.344-200.345 even if an award is terminated in whole or in part. To the extent that subawards are permitted under this NOFO, pass-through entities should refer to 2 C.F.R. § 200.340 for additional information on termination regarding subawards.

a. *Noncompliance*

If a recipient fails to comply with the terms and conditions of a federal award, FEMA may terminate the award in whole or in part. If the noncompliance can be corrected, FEMA may first attempt to direct the recipient to correct the noncompliance. This may take the form of a Compliance Notification. If the noncompliance cannot be corrected or the recipient is non-responsive, FEMA may proceed with a Remedy Notification, which could impose a remedy for noncompliance per 2 C.F.R. § 200.339, including termination. Any action to terminate based on noncompliance will follow the requirements of 2 C.F.R. §§ 200.341-200.342 as well as the requirement of 2 C.F.R. § 200.340(c) to report in FAPIIS the recipient's material failure to comply with the award terms and conditions. See also the section on Actions to Address Noncompliance in this NOFO.

b. *With the Consent of the Recipient*

FEMA may also terminate an award in whole or in part with the consent of the recipient, in which case the parties must agree upon the termination conditions, including the effective date, and in the case of partial termination, the portion to be terminated.

c. *Notification by the Recipient*

The recipient may terminate the award, in whole or in part, by sending written notification to FEMA setting forth the reasons for such termination, the effective date, and in the case of partial termination, the portion to be terminated. In the case of partial termination, FEMA may determine that a partially terminated award will not accomplish the purpose of the federal award, so FEMA may terminate the award in its entirety. If that occurs, FEMA will follow the requirements of 2 C.F.R. §§ 200.341-200.342 in deciding to fully terminate the award.

2. Program Evaluation

Federal agencies are required to structure NOFOs that incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards meeting agency priority goal(s) and program outcomes.

[OMB Memorandum M-21-27](#), Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans, implementing Title I of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019) (Evidence Act), urges federal awarding agencies to use program evaluation as a critical tool to learn, improve equitable 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).

As such, recipients and subrecipients are required to participate in a DHS-, Component, or Program Office-led evaluation if selected, which may be carried out by a third-party on behalf of the DHS, its component agencies, or the Program Office. Such an evaluation may involve information collections including but not limited to surveys, interviews, or discussions with individuals who benefit from the federal award program operating personnel, and award recipients, as specified in a DHS-, component agency-, or Program Office-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). 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.

3. Period of Performance Extensions

Extensions to the period of performance (POP) for this program are allowed. Extensions to the POP identified in the award will only be considered through formal, written requests to the recipient’s FEMA Preparedness Officer and must contain specific and compelling justifications as to why an extension is required. Recipients are advised to coordinate with the FEMA Preparedness Officer as needed when preparing an extension request.

All extension requests must address the following:

- a. The grant program, fiscal year, and award number;

- b. Reason for the delay –including details of the legal, policy, or operational challenges that prevent the final outlay of awarded funds by the deadline;
- c. Current status of the activity(ies);
- d. Approved POP termination date and new project completion date;
- e. Amount of funds drawn down to date;
- f. Remaining available funds, both federal and, if applicable, non-federal;
- g. Budget outlining how remaining federal and, if applicable, non-federal funds will be expended;
- h. Plan for completion, including milestones and timeframes for achieving each milestone and the position or person responsible for implementing the plan for completion; and
- i. Certification that the activity(ies) will be completed within the extended POP without any modification to the original statement of work, as described in the IJ and as approved by FEMA.

Extension requests will be granted only due to compelling legal, policy, or operational challenges. Extension requests will only be considered for the following reasons:

- Contractual commitments by the recipient or subrecipient with vendors prevent completion of the project, including delivery of equipment or services, within the existing POP;
- The project must undergo a complex environmental review that cannot be completed within the existing POP;
- Projects are long-term by design, and therefore acceleration would compromise core programmatic goals; or
- Where other special or extenuating circumstances exist.

Recipients should submit all proposed extension requests to FEMA for review and approval at least 120 days prior to the end of the POP to allow sufficient processing time. Extensions are typically granted for no more than a six-month period.

4. Disability Integration

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

Grant and cooperative agreement recipients should engage with the whole community to advance individual and community preparedness and to work as a nation to build and sustain resilience. In doing so, recipients are encouraged to consider the needs of individuals with disabilities into the activities and projects funded by the grant or cooperative agreement.

FEMA expects that the integration of the needs of people with disabilities will occur at all levels, including planning; alerting, notification, and public outreach; training; purchasing of equipment and supplies; protective action implementation; and exercises/drills.

The following are examples that demonstrate the integration of the needs of people with disabilities in carrying out FEMA awards:

- Include representatives of organizations that work with/for people with disabilities on planning committees, work groups and other bodies engaged in development and implementation of the grant programs and activities.
- Hold all activities related to the grant in locations that are accessible to persons with physical disabilities and intellectual disabilities to the extent practicable.
- Provide auxiliary aids and services, including American Sign Language interpreters, that provide public information across the community and in shelters.
- Ensure shelter-specific grant funds are in alignment with FEMA's [Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters](#).
- If making alterations to an existing building to a primary function area utilizing federal funds, complying with the most recent codes and standards and making path of travel to the primary function area accessible to the greatest extent possible.
- Implement specific procedures used by public transportation agencies that include evacuation and passenger communication plans and measures for individuals with disabilities.
- Identify, create, and deliver training to address any training gaps specifically aimed toward whole-community preparedness. Include and interact with individuals with disabilities, aligning with the designated program capability.
- Establish best practices in inclusive planning and preparedness that consider physical access, needs of individuals with intellectual disabilities, and information access.

FEMA grant recipients can fund projects towards the resiliency of the whole community, including people with disabilities, such as training, outreach and safety campaigns, provided that the project aligns with this NOFO and the terms and conditions of the award.

5. Conflicts of Interest in the Administration of Federal Awards or Subawards

For conflicts of interest under grant-funded procurements and contracts, refer to the section on Procurement Integrity in this NOFO and 2 C.F.R. §§ 200.317 – 200.327.

To eliminate and reduce the impact of conflicts of interest in the subaward process, recipients and pass-through entities must follow their own policies and procedures regarding the elimination or reduction of conflicts of interest when making subawards. Recipients and pass-through entities are also required to follow any applicable federal and state, local, tribal, or territorial (SLTT) statutes or regulations governing conflicts of interest in the making of subawards.

The recipient or pass-through entity must disclose to the respective Preparedness Officer or Program Manager, in writing, any real or potential conflict of interest that may arise during the administration of the federal award, as defined by the federal or SLTT statutes or regulations or their own existing policies, within five days of learning of the conflict of interest. Similarly, subrecipients, whether acting as subrecipients or as pass-through entities, must disclose any real or potential conflict of interest to the recipient or next-level pass-

through entity as required by the recipient or pass-through entity's conflict of interest policies, or any applicable federal or SLTT statutes or regulations.

Conflicts of interest may arise during the process of FEMA making a federal award in situations where an employee, officer, or agent, any members of his or her immediate family, his or her partner has a close personal relationship, a business relationship, or a professional relationship, with an applicant, subapplicant, recipient, subrecipient, or FEMA employees.

6. Procurement Integrity

Through audits conducted by the DHS Office of Inspector General (OIG) and FEMA grant monitoring, findings have shown that some FEMA recipients have not fully adhered to the proper procurement requirements at 2 C.F.R. §§ 200.317 – 200.327 when spending grant funds. Anything less than full compliance with federal procurement requirements jeopardizes the integrity of the grant as well as the grant program. 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), such as the [PDAT Field Manual](#) and [Contract Provisions Guide](#). Additional resources, including an upcoming trainings schedule can be found on the PDAT Website: <https://www.fema.gov/grants/procurement>.

The below highlights the federal procurement requirements for FEMA recipients when procuring goods and services with federal grant funds. FEMA will include a review of recipients' procurement practices as part of the normal monitoring activities. **All procurement activity must be conducted in accordance with federal procurement standards at 2 C.F.R. §§ 200.317 – 200.327.** Select requirements under these standards are listed below. The recipient and any of its subrecipients must comply with all requirements, even if they are not listed below.

Under 2 C.F.R. § 200.317, when procuring property and services under a federal award, states (including territories) must follow the same policies and procedures they use for procurements from their non-federal funds; additionally, states must now follow 2 C.F.R. § 200.321 regarding socioeconomic steps, 200.322 regarding domestic preferences for procurements, 200.323 regarding procurement of recovered materials, and 2 C.F.R. § 200.327 regarding required contract provisions.

All other non-federal entities, such as tribes (collectively, non-state entities), must have and use their own documented procurement procedures that reflect applicable SLTT laws and regulations, provided that the procurements conform to applicable federal law and the standards identified in 2 C.F.R. Part 200. These standards include, but are not limited to, providing for full and open competition consistent with the standards of 2 C.F.R. § 200.319 and the required procurement methods at § 200.320.

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

States are required to follow the socioeconomic steps in soliciting small and minority businesses, women's business enterprises, and labor surplus area firms per 2 C.F.R. §

200.321. All non-federal entities should also, to the greatest extent practicable under a federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States per 2 C.F.R. § 200.322. More information on OMB's revisions to the federal procurement standards can be found in [Purchasing Under a FEMA Award: OMB Revisions Fact Sheet](#).

The recognized procurement methods in 2 C.F.R. § 200.320 have been reorganized into informal procurement methods, which include micro-purchases and small purchases; formal procurement methods, which include sealed bidding and competitive proposals; and noncompetitive procurements. The federal micro-purchase threshold is currently \$10,000, and non-state entities may use a lower threshold when using micro-purchase procedures under a FEMA award. If a non-state entity wants to use a micro-purchase threshold higher than the federal threshold, it must follow the requirements of 2 C.F.R. § 200.320(a)(1)(iii)-(v). The federal simplified acquisition threshold is currently \$250,000, and a non-state entity may use a lower threshold but may not exceed the federal threshold when using small purchase procedures under a FEMA award. See 2 C.F.R. § 200.1 (citing the definition of simplified acquisition threshold from [48 C.F.R. Part 2, Subpart 2.1](#)).

See 2 C.F.R. §§ 200.216, 200.471, and Appendix II as well as section D.13.a of the NOFO regarding prohibitions on covered telecommunications equipment or services.

b. *Competition and Conflicts of Interest*

Among the requirements of 2 C.F.R. § 200.319(b) applicable to all non-federal entities other than states, in order to ensure objective contractor performance and eliminate unfair competitive advantage, 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. FEMA considers these actions to be an organizational conflict of interest and interprets this restriction as applying to contractors that help a non-federal entity 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 non-federal entity.

Under this prohibition, unless the non-federal entity 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.

Additionally, some of the 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;
- Organizational conflicts of interest;
- 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.

Per 2 C.F.R. § 200.319(c), non-federal entities other than states must conduct procurements in a manner that prohibits the use of statutorily or administratively imposed SLTT geographical preferences in the evaluation of bids or proposals, except in those cases where applicable federal statutes expressly mandate or encourage geographic preference. Nothing in this section preempts state licensing laws. When contracting for architectural and engineering services, geographic location may be a selection criterion provided its application leaves an appropriate number of qualified firms, given the nature and size of the project, to compete for the contract.

Under 2 C.F.R. § 200.318(c)(1), non-federal entities other than states 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 non-federal entity may neither solicit nor accept gratuities, favors, or anything of monetary value from contractors or parties to subcontracts. However, non-federal entities may set standards for situations in which the financial interest is not substantial, or the gift is an unsolicited item of nominal value. The standards of conduct must provide for disciplinary actions to be applied for violations of such standards by officers, employees, or agents of the non-federal entity.

Under 2 C.F.R. 200.318(c)(2), if the recipient or subrecipient (other than states) has a parent, affiliate, or subsidiary organization that is not a state, local, tribal, or territorial government, the non-federal entity must also maintain written standards of conduct covering organizational conflicts of interest. In this context, organizational conflict of interest means that because of a relationship with a parent company, affiliate, or subsidiary organization, the non-federal entity is unable or appears to be unable to be

impartial in conducting a procurement action involving a related organization. The non-federal entity must disclose in writing any potential conflicts of interest to FEMA or the pass-through entity in accordance with applicable FEMA policy.

c. *Supply Schedules and Purchasing Programs*

Generally, a non-federal entity may seek to procure goods or services from a federal supply schedule, state supply schedule, or group purchasing agreement.

I. GENERAL SERVICES ADMINISTRATION SCHEDULES

States, tribes, and local governments, and any instrumentality thereof (such as local education agencies or institutions of higher education) may procure goods and services from a General Services Administration (GSA) schedule. GSA offers multiple efficient and effective procurement programs for state, tribal, and local governments, and instrumentalities thereof, to purchase products and services directly from pre-vetted contractors. The GSA Schedules (also referred to as the Multiple Award Schedules and the Federal Supply Schedules) are long-term government-wide contracts with commercial firms that provide access to millions of commercial products and services at volume discount pricing.

Information about GSA programs for states, tribes, and local governments, and instrumentalities thereof, can be found at <https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/buy-from-mas-information-technology/state-and-local-government-ordering> and <https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-buyers/state-and-local-governments>.

For tribes, local governments, and their instrumentalities that purchase off of a GSA schedule, this will satisfy the federal requirements for full and open competition provided that the recipient follows the GSA ordering procedures; however, tribes, local governments, and their instrumentalities will still need to follow the other rules under 2 C.F.R. §§ 200.317 – 200.327, such as solicitation of minority businesses, women’s business enterprises, small businesses, or labor surplus area firms (§ 200.321), domestic preferences (§ 200.322), contract cost and price (§ 200.324), and required contract provisions (§ 200.327 and Appendix II).

II. OTHER SUPPLY SCHEDULES AND PROGRAMS

For non-federal entities other than states, such as tribes, local governments, and nonprofits, that want to procure goods or services from a state supply schedule, cooperative purchasing program, or other similar program, in order for such procurements to be permissible under federal requirements, the following must be true:

- The procurement of the original contract or purchasing schedule and its use by the non-federal entity complies with state and local law, regulations, and written procurement procedures;

- The state or other entity that originally procured the original contract or purchasing schedule entered into the contract or schedule with the express purpose of making it available to the non-federal entity and other similar types of entities;
- The contract or purchasing schedule specifically allows for such use, and the work to be performed for the non-federal entity falls within the scope of work under the contract as to type, amount, and geography;
- The procurement of the original contract or purchasing schedule complied with all the procurement standards applicable to a non-federal entity other than states under at 2 C.F.R. §§ 200.317 – 200.327; and
- With respect to the use of a purchasing schedule, the non-federal entity must follow ordering procedures that adhere to applicable state, tribal, and local laws and regulations and the minimum requirements of full and open competition under 2 C.F.R. Part 200.

If a non-federal entity other than a state seeks to use a state supply schedule, cooperative purchasing program, or other similar type of arrangement, FEMA recommends the recipient discuss the procurement plans with its Grants Management Specialist via the AAD Help Desk at ASK-GMD@fema.dhs.gov.

d. *Procurement Documentation*

Per 2 C.F.R. § 200.318(i), non-federal entities other than states and territories 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 territories are encouraged to maintain and retain this information as well and 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 but are not limited to:

- 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.
- Additional information on required procurement records can be found on pages 24-26 of the [PDAT Field Manual](#).

7. Financial Assistance Programs for Infrastructure

a. *Build America, Buy America Act*

Recipients and subrecipients must comply with 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 and Office of Management and Budget (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.

For FEMA's official policy on BABAA, please see FEMA Policy 207-22-0001: Buy American Preference in FEMA Financial Assistance Programs for Infrastructure available at https://www.fema.gov/sites/default/files/documents/fema_build-america-buy-america-act-policy.pdf. To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to include a Buy America preference, please see [Programs and Definitions: Build America, Buy America Act | FEMA.gov](#) and https://www.fema.gov/sites/default/files/documents/fema_build-america-buy-america-act-policy.pdf.

b. Waivers

When necessary, recipients (and subrecipients through their pass-through entity) may apply for, and FEMA may grant, a waiver from these requirements.

A waiver of the domestic content procurement preference may be granted by the agency awarding official if FEMA 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.
- 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%.

For FEMA awards, the process for requesting a waiver from the Buy America preference requirements can be found on FEMA's website at: ["Buy America" Preference in FEMA Financial Assistance Programs for Infrastructure | FEMA.gov](https://www.fema.gov/buy-america).

c. Definitions

For BABAA specific definitions, please refer to the FEMA Buy America website at: ["Programs and Definitions: Build America, Buy America Act | FEMA.gov"](https://www.fema.gov/buy-america).

Please refer to the applicable DHS Standard Terms & Conditions for the BABAA specific term applicable to all FEMA financial assistance awards for infrastructure.

8. Record Retention

a. 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, FEMA 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. These include:

- Records for real property and equipment acquired with Federal funds must be retained for **three years after final disposition of the property**. *See* 2 C.F.R. § 200.334(c).
- If any litigation, claim, or audit is started before the expiration of the three-year period, the records **must be retained until** all litigation, claims, or audit findings involving the records **have been resolved and final action taken**. *See* 2 C.F.R. § 200.334(a).
- The **record retention period will be extended if the non-federal entity is notified in writing** of the extension by FEMA, the cognizant or oversight agency for audit, or the cognizant agency for indirect costs, or pass-through entity. *See* 2 C.F.R. § 200.334(b).
- Where FEMA requires recipients to report program income after the period of performance ends, the **program income record retention period begins at the end of the recipient's fiscal year in which program income is earned**. *See* 2 C.F.R. § 200.334(e).
- For indirect cost rate computations and proposals, cost allocation plans, or any similar accounting computations of the rate at which a particular group of costs is chargeable (such as computer usage chargeback rates or composite fringe benefit rates), the start of the record retention period depends on whether the indirect cost rate documents were submitted for negotiation. If the **indirect cost rate documents were submitted for negotiation, the record retention period begins from the date those documents were submitted** for negotiation. If indirect cost rate documents were **not submitted for negotiation, the record retention period begins at the end of the recipient's fiscal year or other**

accounting period covered by that indirect cost rate. See 2 C.F.R. § 200.334(f).

b. *Types of Records to Retain*

FEMA requires that non-federal entities 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.

Non-federal entities should keep detailed records of all transactions involving the grant. FEMA may at any time request copies of any relevant documentation and records, including purchasing documentation along with copies of cancelled checks for verification. See, e.g., 2 C.F.R. §§ 200.318(i), 200.334, 200.337.

In order for any cost to be allowable, it must be adequately documented per 2 C.F.R. § 200.403(g). Non-federal entities who fail to fully document all purchases may find their expenditures questioned and subsequently disallowed.

9. *Actions to Address Noncompliance*

Non-federal entities receiving financial assistance funding from FEMA 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, FEMA or the pass-through entity may discover potential or actual noncompliance on the part of a recipient or subrecipient. This potential or actual noncompliance may be discovered through routine monitoring, audits, civil rights complaint investigations and compliance reviews, closeout, or reporting from various sources.

In the case of any potential or actual noncompliance, FEMA may place special conditions on an award per 2 C.F.R. §§ 200.208 and 200.339, FEMA 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. Parts 7 and 19 or other applicable regulations.

In the event the noncompliance is not able to be corrected by imposing additional conditions or the recipient or subrecipient refuses to correct the matter, FEMA may take other remedies allowed under 2 C.F.R. § 200.339. These remedies include actions to disallow costs, recover funds, wholly or partly suspend or terminate the award, initiate suspension and debarment proceedings, withhold further federal awards, or take other remedies that may be legally

available. For further information on termination due to noncompliance, see the section on Termination Provisions in the NOFO.

FEMA may discover and take action on noncompliance even after an award has been closed. The closeout of an award does not affect FEMA's right to disallow costs and recover funds as long as the action to disallow costs takes place during the record retention period. *See* 2 C.F.R. §§ 200.334, 200.345(a). Closeout also does not affect the obligation of the non-federal entity to return any funds due as a result of later refunds, corrections, or other transactions. 2 C.F.R. § 200.345(a)(2).

The types of funds FEMA may attempt to recover include, but are not limited to, improper payments, cost share reimbursements, program income, interest earned on advance payments, or equipment disposition amounts.

FEMA may seek to recover disallowed costs through a Notice of Potential Debt Letter, a Remedy Notification, or other letter. The document will describe the potential amount owed, the reason why FEMA is recovering the funds, the recipient's appeal rights, how the amount can be paid, and the consequences for not appealing or paying the amount by the deadline.

If the recipient neither appeals nor pays the amount by the deadline, the amount owed will become final. Potential consequences if the debt is not paid in full or otherwise resolved by the deadline include the assessment of interest, administrative fees, and penalty charges; administratively offsetting the debt against other payable federal funds; and transferring the debt to the U.S. Department of the Treasury for collection.

FEMA notes the following common areas of noncompliance for FEMA's grant programs:

- Insufficient documentation and lack of record retention.
- Failure to follow the procurement under grants requirements.
- Failure to submit closeout documents in a timely manner.
- Failure to follow EHP requirements.
- Failure to comply with the POP deadline.

10. 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. Recipients and subrecipients must retain award documents for at least three years from the date the final FFR is submitted, and even longer in many cases subject to the requirements of 2 C.F.R. § 200.334. In the case of administrative closeout, documents must be retained for at least three years from the date of closeout, or longer subject to the requirements of 2 C.F.R. § 200.334. If documents are retained longer than the required retention period, the DHS OIG, the GAO, and the pass-through entity, as well as FEMA in its oversight capacity, have the right to access these records as well. *See* 2 C.F.R. §§ 200.334, 200.337.

Additionally, non-federal entities must comply with the single audit requirements at 2 C.F.R. Part 200, Subpart F. Specifically, non-federal entities, other than for-profit subrecipients, that expend \$750,000 or more in federal awards during their fiscal year must have a single or program-specific audit conducted for that year in accordance with Subpart F. 2 C.F.R. § 200.501. A single audit covers all federal funds expended during a fiscal year, not just FEMA funds. The cost of audit services may be allowable per 2 C.F.R. § 200.425, but non-federal entities must select auditors in accordance with 2 C.F.R. § 200.509, including following the proper procurement procedures. For additional information on single audit reporting requirements, see section F of this NOFO under the header “Single Audit Report” within the subsection “Additional Reporting Requirements”.

The objectives of single audits are to:

- Determine if financial statements conform to generally accepted accounting principles (GAAP);
- Determine whether the schedule of expenditures of federal awards is presented fairly;
- Understand, assess, and test the adequacy of internal controls for compliance with major programs; and
- Determine if the entity complied with applicable laws, regulations, and contracts or grants.

For single audits, the auditee is required to prepare financial statements reflecting its financial position, a schedule of federal award expenditures, and a summary of the status of prior audit findings and questioned costs. The auditee also is required to follow up and take appropriate corrective actions on new and previously issued but not yet addressed audit findings. The auditee must prepare a corrective action plan to address the new audit findings. 2 C.F.R. §§ 200.508, 200.510, 200.511.

Non-federal entities must have an audit conducted, either single or program-specific, of their financial statements and federal expenditures annually or biennially pursuant to 2 C.F.R. § 200.504. Non-federal entities must also follow the information submission requirements of 2 C.F.R. § 200.512, including submitting the audit information to the [Federal Audit Clearinghouse](#) within the earlier of 30 calendar days after receipt of the auditor’s report(s) or nine months after the end of the audit period. The audit information to be submitted include the data collection form described at 2 C.F.R. § 200.512(c) and Appendix X to 2 C.F.R. Part 200 as well as the reporting package described at 2 C.F.R. § 200.512(b).

The non-federal entity must retain one copy of the data collection form and one copy of the reporting package for three years from the date of submission to the Federal Audit Clearinghouse. 2 C.F.R. § 200.512; *see also* 2 C.F.R. § 200.517 (setting requirements for retention of documents by the auditor and access to audit records in the auditor’s possession).

FEMA, the DHS OIG, the GAO, and the pass-through entity (if applicable), as part of monitoring or as part of an audit, may review a non-federal entity’s compliance with the single audit requirements. In cases of continued inability or unwillingness to have an audit conducted in compliance with 2 C.F.R. Part 200, Subpart F, FEMA and the pass-through

entity, if applicable, are required to take appropriate remedial action under 2 C.F.R. § 200.339 for noncompliance, pursuant to 2 C.F.R. § 200.505.

11. Payment Information

FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients.

Payment requests are submitted through FEMA GO.

12. Whole Community Preparedness

Preparedness is a shared responsibility that calls for the involvement of everyone—not just the government—in preparedness efforts. By working together, everyone can help keep the nation safe from harm and help keep it resilient when struck by hazards, such as natural disasters, acts of terrorism, and pandemics.

[Whole Community](#) includes:

- Individuals and families, including those with access and functional needs;
- Businesses;
- Faith-based and community organizations;
- Nonprofit groups;
- Schools and academia;
- Media outlets; and
- All levels of government, including state, local, tribal, territorial, and federal partners.

The phrase “Whole Community” often appears in preparedness materials, as it is one of the guiding principles. It means two things:

1. Involving people in the development of national preparedness documents.
2. Ensuring their roles and responsibilities are reflected in the content of the materials.

13. Report issues of fraud, waste, abuse

Please note, when applying to this notice of funding opportunity and when administering the grant, applicants may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct 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.

14. Continuity Capability

Continuity should be integrated into each core capability and the coordinating structures that provide them. Protection of critical systems and networks that ensure continuity of operation, business and government are fundamental to ensuring the delivery of all core capabilities. Continuity capabilities increase resilience and the probability that organizations can perform essential functions in the delivery of core capabilities that support the mission areas. FEMA is responsible for developing, managing, and promulgating national continuity planning, guidance, training, and exercise programs for the whole community.

FEMA develops and promulgates directives, policy, and guidance for continuing SLT government jurisdictions, nongovernmental organizations, and private sector organizations’

essential functions across a broad spectrum of emergencies. This direction and guidance assist in developing capabilities for continuing the essential functions of SLT governmental entities, as well as public/private critical infrastructure owners, operators, and regulators enabling them.

Continuity Guidance Circular outline continuity requirements for agencies and organizations and provide guidance, methodology, and checklists. For additional information on continuity programs, guidance, and directives, visit the Continuity Resource Toolkit at <https://www.fema.gov/emergency-managers/national-preparedness/continuity>. For additional information on continuity programs, guidance, and directives, visit <https://www.fema.gov/emergency-managers/national-preparedness/continuity/circular>.

This aligns with the requirements that approved Cybersecurity Plans ensure continuity of operations of the state or territory as well as applicable local governments in the event of a cybersecurity incident, as well as continuity of communications and data networks within the state or territory and between the state or territory and applicable local governments. 6 U.S.C. § 665g(e)(2)(B)(vii), (ix).

15. Hazard-Resistant Building Codes

Hazard-resistant building codes are a foundational element of a more resilient nation, safeguarding communities and lives against natural disasters, with an estimated \$11:1 return on investment. The adoption, enforcement and application of modern building codes mitigates community vulnerabilities, reduces disaster recovery costs, and strengthens nationwide capability. FEMA is working to promote and support building codes in all areas of its work in support of the multi-agency National Initiative to Advance Building Codes. In the interest of building a stronger, more resilient nation, FEMA encourages all grant recipients and subrecipients to meet current published editions of relevant consensus-based building codes, specifications and standards, and to exceed them where feasible.

16. Appendices

- Appendix A. Program Goals and Objectives
- Appendix B. Cybersecurity Planning Committee and Charter
- Appendix C. Cybersecurity Plan
- Appendix D. POETE Solution Areas for Investments
- Appendix E. SLCGP Requirements Matrix
- Appendix F. Required, Encouraged, and Optional Services, Memberships, and Resources

Appendix A: Program Goals and Objectives

Our nation faces unprecedented cybersecurity risk due to increasingly sophisticated adversaries that threaten critical infrastructure, widespread vulnerabilities in commonly used software and hardware, and broad dependencies on networked technologies for the delivery of National Critical Functions, the disruption of which would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Cyber risk management is particularly complex due to several factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities in cyber infrastructure. Considering the risk and potential consequences of cyber incidents, particularly to [critical infrastructure sectors](#), strengthening the cybersecurity practices and resilience of SLT governments is an important homeland security mission.

As part of DHS, CISA is at the heart of mobilizing a collective defense to understand and manage risk to our critical infrastructure partners. In its unique role, CISA is proactively supporting efforts to achieve a cybersecurity ecosystem in which malicious actors face insurmountably high costs to execute damaging intrusions, vulnerabilities are rapidly identified before exploitation, and technology is used to reduce the most harmful and systemic risks to critical infrastructure. CISA programs and services are driven by a comprehensive understanding of the risk environment and the corresponding needs identified by our partners. The SLCGP is key to achieving this vision and enables DHS to make targeted investments in SLT government agencies, improving the security and resilience of critical infrastructure upon which Americans rely.

The goals and objectives outlined below, if achieved, will significantly reduce the risk of a cybersecurity threat against SLT government information technology (IT) networks. These broad outcomes are listed in logical sequence to aid recipients in focusing on the overall intent of the SLCGP. These outcomes will help prioritize the use of scarce resources and to develop metrics to gauge success at both the project and organizational level. Outcomes of the program will be measured by how well recipients can achieve outlined goals and improve the risk posture of the information systems they either own or those that are operated on their behalf.

The program objectives for SLCGP are as follows: (1) develop and establish appropriate governance structures, as well as develop, implement, or revise Cybersecurity Plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations; (2) ensure SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments; (3) implement security protections commensurate with risk (outcomes of SLCGP Objectives 1 & 2); and (4) ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities. These program objectives are further divided into sub-objectives and outcomes with accompanying sample evidence of implementation provided to assist the reader in development of their application.

Goal of SLCGP: Assist SLT governments with managing and reducing systemic cyber risk.

(You have met Objective 1 if you are an SLT that has successfully applied and received approval of all requirements for FY 2022/2023.)

Program Objective	Program Sub-Objective(s)	Outcome(s)	Evidence of Implementation Example
1. Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations	1.1: Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and the National Institute of Standards and Technology (NIST).	1.1.1 Participants have established and documented a uniform cybersecurity governance structure that is accountable to organizational leadership and works together to set the vision for cyber risk management. 1.1.2 Participants have identified senior officials to enable whole-of organization coordination on cybersecurity policies, processes and procedures.	Organization has a cybersecurity defense concept of operations, with responsibilities assigned to specific organizational roles.
	1.2 Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.	1.2.1 Develop, implement, or revise and exercise cyber incident response plans.	Organization conducts annual table-top and full-scope exercises that include practical execution of restoration and recovery processes to test approved cybersecurity plans. Conducting these exercises allow organizations to test approved cybersecurity plans to identify, protect, detect, respond to and recover from cybersecurity incidents, in line with the NIST Cybersecurity Framework, and demonstrates process to incorporate lessons learned from the exercise into their cybersecurity program.
	1.3 Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset's criticality and business value.	1.3.1 Ensure that systems and network functions are prioritized and reconstituted according to their impact to essential functions.	Organization conducts a regular business impact assessment to prioritize which systems must be protected and recovered first.

Program Goals	Program Objectives	Outcome(s)	Evidence of Implementation Example
2. SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation and structured assessments	2.1 Physical devices and systems, as well as software platforms and applications, are inventoried.	2.1.1 Establish and regularly update asset inventory.	Organization maintains and regularly updates an asset inventory list.
	2.2 Cybersecurity risk to the organization's operations and assets are understood.	2.2.1 Conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement.	Organization annually completes the Nationwide Cybersecurity Review (NCSR).
	2.3 Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.	2.3.1 Participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program. 2.3.2 Effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.	Organization is an active participant in CISA's Cyber Hygiene program. Organization has a plan to manage vulnerabilities based on those with the highest criticality, internet-facing vulnerabilities, as well as known exploited vulnerabilities identified in CISA's Known Exploited Vulnerabilities Catalog.
	2.4 Capabilities are in place to monitor assets to identify cybersecurity events.	2.4.1 SLT agencies are able to analyze network traffic and activity transiting or traveling to or from information systems, applications, and user accounts to understand baseline activity and identify potential threats.	<i>Not Applicable</i>
	2.5 Processes are in place to action insights derived from deployed capabilities.	2.5.1 SLT agencies are able to respond to identified events and incidents, document root cause, and share information with partners.	<i>Not Applicable</i>

Program Goals	Program Objectives	Outcome(s)	Evidence of Implementation Example
3. Implement security protections commensurate with risk (Outcomes of goals 1 & 2)	3.1 SLT agencies adopt fundamental cybersecurity best practices.	3.1.1 Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.	The organization implements MFA for all remote access and privileged accounts.
	3.2 Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.	3.2.1 Individual participants address items identified through assessments and planning process 3.2.2 SLT entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional and intra-state efforts).	<i>Not Applicable</i>
Program Goals	Program Objectives	Outcome(s)	Evidence of Implementation Example
4. Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.	4.1 Train personnel to have the fundamental knowledge and skills necessary to recognize cybersecurity risks and understand their roles and responsibilities within established cybersecurity policies, procedures, and practices.	4.1.1 Organization requires regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees. 4.1.2 Organization has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.	<i>Not Applicable</i>
	4.2 Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.	4.2.1 Organization has established cyber workforce development and training plans, based on the NICE Cybersecurity Workforce Framework.	<i>Not Applicable</i>

Appendix B: Cybersecurity Planning Committee and Charter

Governance

In keeping with the guiding principles of governance for all DHS preparedness programs and statutory requirements, recipients must coordinate activities across preparedness disciplines and levels of government, including SLT governments. Specific attention should be paid to how available funding sources can effectively support a whole of state approach to cyber preparedness and resiliency. To ensure this, in FY 2022, the entity must have established or reestablished a Cybersecurity Planning Committee. A Cybersecurity Planning Committee is also required pursuant to the statute authorizing the SLCGP (see section 2220A(g) of the Homeland Security Act of 2002, as amended (6 U.S.C. § 665g(g))).

In FY 2024, the resubmission of Cybersecurity Planning Committee membership and Charter is not required. Applicants are still encouraged to provide any updated membership and bylaws as applicable in the application.

Cybersecurity Planning Committee

The Cybersecurity Planning Committee builds upon previously established advisory bodies under other preparedness grant programs. The membership of the Cybersecurity Planning Committee must reflect an eligible entity's unique cybersecurity risk profile.

An existing multijurisdictional planning committee must meet the membership requirements as outlined in the next section, or an existing committee's membership can be expanded or leveraged to meet the membership requirements as well as the unique requirements of each eligible entity. It is recommended that eligible entities consider using Senior Advisory Committees or create a subcommittee within an existing multijurisdictional committee for this purpose, modified to meet the membership and purpose requirements. Any reference to a Cybersecurity Planning Committee elsewhere in this notice, and the accompanying requirements, also apply to these alternative planning committee options.

Cybersecurity Planning Committee Composition and Scope Requirements

Cybersecurity Planning Committee membership must include at least one representative from each of the stakeholders below:

- The eligible entity;
- The CIO, the 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.

At least one half of the representatives of the approved Cybersecurity Planning Committee must have professional experience relating to cybersecurity or information technology. Qualifications are determined by the states.

DHS strongly encourages membership from critical infrastructure sectors and subsectors including K-12 education, water/wastewater, healthcare, energy, defense, and elections infrastructure. Eligible entities are given the flexibility to identify the specific public health and public education representatives to include in the committee.

DHS strongly encourages eligible entities to consider naming additional members to the approved Cybersecurity Planning Committee, including but not limited to representatives from the following:

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

The composition, structure, and charter of the approved Cybersecurity Planning Committee should focus on building cybersecurity capabilities across the eligible entity instead of simply combining previously existing advisory bodies under other grant programs. Eligible entities should continue to verify compliance with Cybersecurity Planning Committee membership requirements and are encouraged to submit updates as appropriate. The below table provides a suggested format for submitting the list of required Cybersecurity Planning Committee members.

Representation	Committee Member Name	Committee Member Title	Committee Member's Organization	Cybersecurity/IT experience (Yes/No)
State or Territory				
Counties, cities, and towns within the jurisdiction of the entity				
Institution of Public Education within the eligible entity				
Institution of Public Health within the eligible entity				
(Additional)				

Representation	Committee Member Name	Committee Member Title	Committee Member's Organization	Cybersecurity/IT experience (Yes/No)
As appropriate, representatives of rural, suburban, and high-population jurisdictions				
(Here the entity may add others at their discretion)				

Cybersecurity Planning Committee Responsibilities

The responsibilities of the approved Cybersecurity Planning Committee include:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Creating a cohesive planning network that builds and implements cybersecurity preparedness initiatives using CISA and FEMA resources, as well as other federal, SLT, private sector, and faith-based community resources;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities, or activities provided by the eligible entity through this program.

Limitations

Cybersecurity Planning Committees that meet the requirements of this NOFO and the statute are not permitted to make decisions relating to information systems owned or operated by, or on behalf of, the state.

Cybersecurity Planning Committee Charter

The governance of the SLCGP through the approved Cybersecurity Planning Committee must be documented in a charter. All members of the Cybersecurity Planning Committee should sign and date the charter showing their agreement with its content and their representation on the committee. Eligible entities should continue to verify compliance with Cybersecurity Planning Committee charter requirements and are encouraged to submit updates as applicable to the recipient's assigned FEMA Preparedness Officer. The Cybersecurity Planning Committee charter must, at a minimum, provide:

- A detailed description of the Cybersecurity Planning Committee's composition and an explanation of key governance processes;
- A description of the frequency at which the Cybersecurity Planning Committee will meet;
- An explanation as to how the committee will leverage existing governance bodies;

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

To ensure ongoing coordination efforts, eligible entities are encouraged to share community preparedness information from other preparedness grant programs as submitted in a state's Biannual Strategy Implementation Report with members of the approved Cybersecurity Planning Committee. Eligible entities are also encouraged to share their Threat and Hazard Identification and Risk Assessment/Stakeholder Preparedness Review data with members of the approved Cybersecurity Planning Committee who are applying for other FEMA preparedness grants to enhance their understanding of statewide capability gaps.

To manage this effort and to further reinforce collaboration and coordination across the stakeholder community, a portion of the 20% funding holdback of a state (including territories) award may be utilized by the eligible entity to support the approved Cybersecurity Planning Committee and to ensure representation and active participation of Cybersecurity Planning Committee members. Funding may be used for hiring and training planners, establishing and maintaining a program management structure, identifying and managing projects, conducting research necessary to inform the planning process, and developing plans that bridge mechanisms, documents, protocols, and procedures.

Appendix C: Cybersecurity Plan

Submission of a Cybersecurity Plan is required for any eligible entity participating in the SLCGP. The Cybersecurity Plan is a key component of a strategic approach to building cyber resilience. The approved Cybersecurity Planning Committee, with a holistic membership representing the various stakeholder groups across the entity, is responsible for developing, approving, revising, and implementing the approved Cybersecurity Plan.

All applicants with a Cybersecurity and Infrastructure Security Agency (CISA)-approved Cybersecurity Plan must submit their current Cybersecurity Plan to CISA via the FEMA SLCGP Inbox at FEMA-SLCGP@fema.dhs.gov no later than January 30, 2025, and annually thereafter on the same date throughout the grant's period of performance. When submitting its Cybersecurity Plan, an applicant must inform CISA whether or not it revised its plan since CISA's last approval of it. If it has revised its Cybersecurity Plan, the applicant must provide a brief explanation of the revisions. There is no requirement for an applicant to revise a Cybersecurity Plan that CISA has approved unless CISA notifies the applicant that the plan does not meet plan requirements.

Eligible applicants must coordinate with the appropriate Cybersecurity and CISA Regional Representatives before submitting their Cybersecurity Plan, Investment Justifications (IJ), and/or Project Worksheet (PW) (See [Section G](#) of this funding notice for relevant contact information). Additionally, all updated plans must be approved by the entity's respective Cybersecurity Planning Committee.

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

At the highest level, the Cybersecurity Plan:

- Provides a comprehensive, strategic plan to reduce cybersecurity risk and increase capability across the entity.
- Encompasses the entire enterprise and is not limited to a single entity.
- Provides strategic direction for two to three years.
- Includes required elements, with discretion to add other elements as necessary.
- Leverages existing plans, to the extent they are in place.
- Aligns individual projects to the Cybersecurity Plan.
- Receives approval from the Cybersecurity Committee and CIO/CISO/equivalent (e.g., Chief Cyber Officer, Governor's cabinet official overseeing cybersecurity).
- Receives CISA review and approval.

In further developing the Cybersecurity Plans, the following is recommended:

- Incorporate existing governance and planning documents and identification of any planning gaps that should be addressed by the Cybersecurity Plan;

- Leverage existing assessments and evaluations (e.g., reports, after action reports) conducted by SLT governments within the entity and any planning gaps that require additional assessments and/or evaluations; and
- Identify potential SLCGP projects to address planning gaps and prioritize mitigation efforts.

Cybersecurity Plan Components

- Roles and responsibilities
- Required elements
- Discretionary elements
- Capabilities assessment
- Implementation plan
- A summary of projects
- Metrics

Cybersecurity Plan Overview

The following identifies the plan requirements and additional considerations that eligible entities should consider when constructing the Cybersecurity Plan and future updates. Although there is no required format for the Cybersecurity Plan, the approved Cybersecurity Planning Committees are encouraged to review the Cybersecurity Plan Template, which includes additional details, samples, and templates.

Cybersecurity Plans must include and address the following items:

- **Incorporate, to the extent practicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLTs.** Building upon and incorporating existing structures and capabilities allows entities to provide governance and a framework to meet the critical cybersecurity needs across the entity while making the best use of available resources. For example, consider referencing an existing emergency management plan to address potential cascading impacts affecting health and safety when responding to or recovering from a cybersecurity incident.
- **Describe how input and feedback from local governments and associations of local governments was incorporated.** For states, the SLCGP is intended to reduce cybersecurity risk across the eligible entity. Incorporating input from local entities is critical to building a holistic Cybersecurity Plan.
- **Include the specific required elements** (see Required Elements section of this Appendix). There are 16 required elements that are central to the Cybersecurity Plan and represent a broad range of cybersecurity capabilities and activities. They also include specific cybersecurity best practices that, when implemented over time, will substantially reduce cybersecurity risk and cybersecurity threats. Although each of the 16 required elements must be addressed in the plan, this may include a brief explanation as to why certain elements are not currently being prioritized. Not all 16 elements are required to be aligned to projects and have associated funding. These determinations should be addressed in accordance with capability gaps and vulnerabilities identified through an objective assessment process.

- **Describe, as appropriate and to the extent practicable, the individual responsibilities of the state and local governments within the state in implementing the Cybersecurity Plan.** Defining the roles and responsibilities of SLT governments is critical from both governance and implementation perspectives.
- **Assess the required elements from an entity-wide perspective.** The candid assessment of the current capabilities of SLT entities is the first step in reducing cybersecurity risk across the entity. This assessment also serves as the justification for individual projects. Additional information on the assessment is provided below and in the Cybersecurity Plan Template, Appendix A, which includes a fillable capabilities assessment chart.
- **Outline, to the extent practicable, the necessary resources and a timeline for implementing the plan.** The Cybersecurity Plan is a strategic planning tool that looks two to three years into the future. Accordingly, it should set forth how the approved Cybersecurity Planning Committee seeks to achieve plan goals and objectives. Cybersecurity Plans should address how SLCGP funds will help develop and/or implement the plan, along with milestones related to major projects. It should also set forth how other activities and funding sources contribute to the achieving the outcomes described in the plans.
- **Summary of associated projects.** Individual projects are the way elements of the plan are implemented over time. The plan must include a summary of projects associated with each required and discretionary element, designating which will use SLCGP funds. Details for each project using SLCGP funds must be included in the IJs.
- **Describe the metrics that the eligible entity will use to measure progress.** The metrics that will be used must measure implementation of the Cybersecurity Plan and, more broadly, cybersecurity risks reduction across the state. **These are different than the metrics that will be used to measure outcomes of the SLCGP, as described in Section A.10, “Performance Measures” of this NOFO.** Additional information is provided in the Cybersecurity Plan Metric Section below and in the Cybersecurity Plan Template.
- **Approvals - the Cybersecurity Plan must be approved by the Cybersecurity Planning Committee and the CIO/CISO/equivalent** (e.g., Chief Cyber Officer, Governor’s cabinet official overseeing cybersecurity). The eligible entity, upon submitting the Cybersecurity Plan, must certify that the Cybersecurity Plan has been formally approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent of the eligible entity.

If resubmitting Cybersecurity Plans by January 30, 2025, applicants should consider providing the following items:

- **Updated signed letter from the entity Cybersecurity Planning Committee.** Initial Cybersecurity Plans included a signed letter from the Cybersecurity Planning Committee, which documented the entity’s commitment to improving cybersecurity and supporting the state or territory government and practitioners across local jurisdictions. An updated letter should include an updated date with language acknowledging the Cybersecurity Planning Committee’s support for this updated plan, and updated signatures.

- **Updated Capabilities Assessment.** The capabilities assessment provides insight into the entity's cybersecurity capabilities across the program elements. Some include the management of information systems, adoption of best practices, continuity of operations, and distribution of funds and services. Through the implementation of SLCGP-funded projects, entities should see improvements in their capabilities in addressing program elements. It should also identify the funding expended in pursuit of enhancing entity capabilities.
- **Updated Implementation Plan.** The Implementation Plan includes information related to the organization, roles, and responsibilities of the entity as it pertains to cybersecurity and the committee. This should be updated as appropriate with new committee members and organizational changes. The Implementation Plan also includes a Resource Overview, a list of resources needed to implement the plan, and a Projected Timeline, which outlines the time it will take to implement the Cybersecurity Plan. The Implementation Plan should be updated to include new information related to the entity's resources and projected timeline to implement the plan and its projects.
- **Updated Project Worksheet.** The Project Worksheet includes all cybersecurity projects the entity plans to pursue through SLCGP and includes the total project cost. During the program, entities have established and made progress on projects with SLCGP funding. This section should be updated with new projects and revised project costs, as applicable.
- **Updated Metrics.** The Metrics section allows entities to list the measures and data being collected to evaluate progress against the SLCGP objectives. Through the duration of the program, the entity has likely made progress on meeting defined metrics and establishing new metrics. As applicable, the entity should update its metrics section with changes made to program goals, and associated metrics as applicable. A CISA metrics menu can be accessed through the entity's CSA/CSC, or directly from CISA through the SLCGP mailbox at SLCGPinfo@cisa.dhs.gov.

Cybersecurity Planning Committees should also consider the following when resubmitting and updating the Cybersecurity Plan:

- **Holistic approach to the Cybersecurity Plan.** The Cybersecurity Plan should be strategic in nature, guiding development of capabilities to address cybersecurity risks and threats across the state or territory. Individual state, territorial, and local entity projects should demonstrably achieve those capabilities over time.
- **Prioritizing projects that address cybersecurity for critical infrastructure.** SLT entities are strongly encouraged to include projects related to K-12 education, water/wastewaters, healthcare, energy, defense, and elections infrastructure.
- **Considering shared services as an effective method in developing projects that address the cybersecurity needs of more than one SLT entity while benefiting from economies of scale.**
- **Focused investments that are sustainable over time.** The SLCGP currently is authorized for four years, and limited funds are available. Entities should consider how to sustain capabilities once the program ends or funds are no longer available.
- **State and territory role as leader and service provider.** Many states and territories have significant cyber defenses and elect to provide services to local entities to improve

capabilities. Where appropriate, states should consider approaches to support state-wide efforts, that may include using funds to provide services to local entities. Multi-entity projects are another way that eligible entities can group together to address cybersecurity risk and build capabilities.

- Building from existing efforts. Cybersecurity Committees should consider describing how cooperative programs developed by groups of local governments are integrated into the entity-wide approach.
- Additional cybersecurity elements prioritized by the approved Cybersecurity Planning Committee.

Required Elements

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The entity's analysis of each element should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below. The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:
 - 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; and
- Migration to the .gov internet domain.

Additional best practices that the Cybersecurity Plan can address include:

- NIST Cybersecurity Framework;
 - NIST's cyber chain supply chain risk management best practices; and
 - Knowledge bases of adversary tools and tactics.
6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
 7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
 8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by National Institute of Science and Technology (NIST) to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
 9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
 10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
 11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
 12. Leverage cybersecurity services offered by the Department (See [Appendix F](#) for additional information on CISA resources and required services and membership).
 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
 14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should

be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

15. Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.

16. Distribute funds, items, services, capabilities, or activities to local governments.

Cybersecurity Planning Committees are strongly encouraged to expand their Cybersecurity Plans beyond the required elements. This may include a focus on specific critical infrastructure or emphasis on different types of SLT entities.

Required Key Cybersecurity Best Practices

Key Cybersecurity Best Practices must be addressed in the Cybersecurity Plan, but immediate adoption by every SLT entity is not required. Cybersecurity Plans must clearly articulate efforts to implement these cybersecurity best practices across the eligible entity within reasonable timelines as funding permits. Cybersecurity Planning Committees should prioritize these best practices in individual projects that assist SLT entities. As there are multiple ways to implement the best practices, this program provides committees the flexibility to work with SLT entities to design a plan that takes resource constraints, existing programs, and other factors into account.

Required Cybersecurity Plan Capabilities Assessment

Given the Cybersecurity Plan is a strategic document, it should not identify specific vulnerabilities but instead capture the broad level of capability across the state or territory. The assessment will become the road map for the state's or territory's individual projects and activities using SLCGP funds. **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.** The Cybersecurity Plan Capabilities Assessment in the Cybersecurity Plan Template provides an easy way for approved Cybersecurity Planning Committees to capture this information and can be customized as appropriate.

Summary of Projects

Although the Cybersecurity Plan is a strategic document, it must show how individual projects and activities will contribute to the implementation of the Plan over time. A summary of projects using FY 2024 SLCGP funds associated with each required and discretionary element provides a helpful snapshot of state- and territory-wide capability and capacity that will be achieved as a result of this funding. Details for each project using SLCGP funds must be included in IJs and are to include a description of the purpose of the project and what it will accomplish, and, more specifically, how the project will address an identified gap or need and how it supports one or more of the required elements.

The Cybersecurity Plan Template includes a fillable Project Plan Worksheet, a sample of which is below.

- Column 1. Project number assigned by the entity

- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Elements the project addresses
- Column 5. Estimated project cost
- Column 6. Status of project (future, ongoing, complete)
- Column 7. Project priority listing (high, medium, low)
- Column 8. Project Type (Plan, Organize, Equip, Train, Exercise)
- Column 9. Activities to accomplish the project with projected dates of completion

Sample Table – Project Plan Worksheet:

1. #	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type	9. Project Milestones

Cybersecurity Plan Metrics

Cybersecurity Plans must include language detailing processes and methods for measuring the following:

- How the state or territory will implement the plan;
- How the state or territory will reduce cybersecurity risks; and
- How the state or territory will identify, respond to, and recover from cybersecurity threats to information systems owned or operated by, or on behalf of, the state or local governments within the state.

These measures should be at the macro level, related to the goals, objectives, and priorities as part of the overarching strategic plan and not associated with individual projects.

The SLCGP SAAs, in partnership with their approved Cybersecurity Planning Committees, should consider the following when developing Cybersecurity Plan metrics:

- Aligning metrics to the Cybersecurity Plan and the established program goals and objectives and state/territory priorities;
- Reviewing existing metrics that are in use across the state or territory;
- Reporting data for each metric that is accurate, timely, accessible and validated; and
- Ensuring that the collection of metric data is not burdensome to the jurisdiction from which it must be obtained.
- Reviewing CISA metrics menu, accessed through the entity's CSA/CSC, or directly from CISA through the SLCGP mailbox at SLCGPinfo@cisa.dhs.gov.

The **Cybersecurity Plan Template** provides a fillable table for reporting metrics.

Sample Table – Cybersecurity Plan Metrics:

Program Objectives	Program Sub Objectives	Associated Metrics	Metric Description (details, source, frequency)
1.	1.1		
	1.2		
	1.3		
2.	2.1		
	2.2		
	2.3		
3.	3.1		
	3.2		
	3.3		
4.	4.1		
	4.2		
	4.3		

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.

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.**

Organization

Organization costs are allowable under this program. States and territories must justify proposed expenditures of SLCGP funds to support organization activities within their IJ and PW 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 [SAFECOM Guidance](#) 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 an already-owned piece of equipment system, 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 POP 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 and/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. Any training or training gaps, including training related to underserved communities (e.g., children, seniors, individuals with disabilities or access and functional needs, individuals with diverse culture and language use, individuals with lower economic capacity and other underserved populations that may be more impacted by disasters) should be identified in the assessment and addressed in the eligible entity's training cycle. 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 (CDP), the Emergency Management Institute (EMI), and FEMA's Training Partner Programs, including the Continuing Training Grants (CTG), the National Domestic Preparedness Consortium (NDPC), the Rural Domestic Preparedness Consortium (RDPC), 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 <https://www.fema.gov/media-library/assets/documents/90195>.

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 Framework. Additional information can be found at <https://fedvte.usalearning.gov>.

Exercises

Exercise costs are allowable under this program. Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP guidance for exercise design, development, conduct, evaluation, and improvement planning is located at <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>.

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 <https://www.fema.gov/media-library/assets/documents/90195>.

Appendix E. SLCGP Requirements Matrix

ID	Category	Requirement	Location	Due Date Cycle	Due Date	Submission Plan
1	Administrative	Pass-through Requirement	NOFO, Sec. G	Within 45 calendar days of release of funds	Varies	Email Certification letter in writing to FEMA Preparedness Officer. A copy will be shared with CISA.
2	Administrative	Rural Pass-through Requirements	NOFO Sec. G	Within 45 Calendar days of release of funds	Varies	Email Certification letter in writing to FEMA Preparedness Officer. A copy will be shared with CISA.
3	Application	Cybersecurity Plan (Resubmissions, if applicable, required by January 30, 2025)	NOFO Sec. A	Prior to award or during POP (if not already approved by CISA)	Varies	Pre-Award-: FEMA GO Post Award: Submit by email to FEMA Preparedness Officer (Password Protected)
4	Application	Cybersecurity Planning Committee Membership List	NOFO Sec. A	Prior to award or during POP (if not already approved by CISA)	Varies	Prior to Award: FEMA GO Post Award: Submit to FEMA Preparedness Officer (Password Protected)
5	Application	Cybersecurity Planning Committee Charter	NOFO Sec. A	Prior to award or during POP (if not already approved by CISA)	Varies	Pre-Award: FEMA GO Post Award: Submit to FEMA Preparedness Officer (Password Protected)
6	Application	Investment Justification	NOFO Sec. A	Prior to award	At time of application	Pre-Award: FEMA GO Post Award: Submit to FEMA Preparedness Officer
7	Application	Project Worksheet	NOFO Sec. A	Prior to award	At time of application	Pre- Award: FEMA GO Post Award: Submit to FEMA Preparedness Officer
8	Financial Closeout	Financial Closeout Reporting Requirements	NOFO Sec. G	Within 120 days after end of POP	Varies	Submit final SF-425 Federal Financial Report (FFR) in PARS; and process final reimbursement requests in PARS
9	Cost Share	Cost Share Requirement	NOFO Sec C	Application, Quarterly, Closeout	Varies	Federal Financial Report (FFR)/SF-425 (Quarterly and at Closeout)
10	Exercises	EHP Review/ Approval	NOFO Sec. F	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	Pre-Award	Pre-award Cost	NOFO Sec. D	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

ID	Category	Requirement	Location	Due Date Cycle	Due Date	Submission Plan
12	Post Award	Cybersecurity Membership (Cyber Hygiene Services)	NOFO Appendix F	Post award	During the first year of the award/sub award POP, and annually	SAA and their subrecipients receiving federal funding; however, subrecipients receiving non-funding assistance in lieu of funding do not have to complete the NCSR.
13	Post Award	Nationwide Cybersecurity Review (NCSR)	NOFO Appendix F	Post Award	During the first year of the award/sub award POP, and annually	SAA and their subrecipients receiving federal funding in the form of a grant award or subgrant award, respectively; however, entities receiving non-funding services, benefits, etc., in lieu of funding, do not have to complete the NCSR. The NCSR is open for submissions from Oct. 1 to the following Feb. 28 annually.
14	Reporting	Standard Form (SF) 425, also known as the Federal Financial Report (FFR)	NOFO Sec. G	Quarterly	30-Jan 30-Apr 30-Jul 30-Oct	Submit SF-425 FFR in the Payment and Reporting Systems (PARS)
15	Progress Reporting and Performance Measurement	Performance Progress Report (PPR) and SAFECOM Certification Letter	NOFO Sec. F & G	Once annually and at Closeout	30-Jan and Closeout	Submit Signed report (PDF) and SAFECOM certification letter in FEMA GO
16	Reporting	Single Audit Report	NOFO Sec. G	Throughout POP	Varies	Federal Audit Clearinghouse https://facweb.census.gov/uploadpdf.aspx

Appendix F: Required, Encouraged, and Optional Services, Memberships, and Resources

All SLCGP recipients and subrecipients that receive funding in the form of a grant, subgrant or benefits of services, activities, etc. in lieu of subgrant funding, are required to participate in a limited number of free services by CISA and the requirement depends on the service. For example, the NCSR is only required for those recipients and subrecipients receiving a grant award or subgrant award. However, 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 and Memberships

<u>Services & Memberships</u>	<u>State government must enroll/ complete?</u>	<u>Local government must enroll/ complete?</u>	<u>Local or state government must enroll/ complete if it receiving benefits, services, etc. in lieu of funding?</u>
Cyber Hygiene (CyHy) services, specifically: <ul style="list-style-type: none"> Vulnerability Scanning (VS) 	Required	Required	Required
Nationwide Cybersecurity Review (NCSR)	Required only if receiving funding in the form of a subgrant award	Required only if receiving funding in the form of a subgrant award	Recommended

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 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 Page](#).

Nationwide Cybersecurity Review (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT’s cybersecurity programs. It is based on the NIST Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Eligible entities and their subrecipients are required to complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually.

For more information, visit [Nationwide Cybersecurity Review \(cisecurity.org\)](https://www.cisecurity.org/nationwide-cybersecurity-review).

All SLCGP recipients are strongly encouraged to participate in other memberships. Additional, optional CISA resources are also available in this Appendix.

Encouraged Services, Membership and Resources

Services & Memberships	State government must enroll/ complete?	Local government must enroll/ complete if it receives funding?	Local government must enroll/ complete if it only receives non-funding assistance?
Multi-State Information Sharing and Analysis Center (MS-ISAC)	Recommended	Recommended	Recommended
Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)	Recommended	Recommended	Recommended

Membership in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and /or Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)

Recipients and subrecipients are strongly encouraged to become a member of the MS-ISAC and/or EI-ISAC, as applicable. Membership is free.

The MS-ISAC receives support from and has been designated by DHS as the cybersecurity ISAC for SLT governments. The MS-ISAC provides services and information sharing that significantly enhances SLT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises. DHS maintains operational-level coordination with the MS-ISAC through the presence of MS-ISAC analysts in CISA Central to coordinate directly with its own 24x7 operations center that connects with SLT government stakeholders on cybersecurity threats and incidents. To register, please visit <https://learn.cisecurity.org/ms-isac-registration>. For more information, visit [MS-ISAC \(cisecurity.org\)](https://www.cisecurity.org/ms-isac).

The EI-ISAC is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council. The EIISAC is funded through DHS grants and offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and

training products. To register, please visit <https://learn.cisecurity.org/ei-isac-registration>. For more information, visit <https://www.cisa.gov/election-security>.

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 Assessment](#)
- [EDM Downloadable Resources](#)
- [Cyber Infrastructure Survey](#)
- [Free Public and Private Sector Cybersecurity Tools and Services](#)
- [Cross-Sector Cybersecurity Performance Goals](#)
- [Web Application Scanning](#)
- [Risk and Vulnerability Assessment - 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](#).

For additional information on memberships, visit [Information Sharing and Analysis Organization \(ISAO\) Standards Organization](#).