The Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program

Release Date: Sep 16, 2022

Download a PDF copy of this webpage.

Effective April 4, 2022, the Federal Government transitioned from using the Data Universal Numbering System or DUNS number, to a new, non-proprietary identifier known as a Unique Entity Identifier or UEI. For entities that have an active registration in the System for Award Management (SAM) prior to this date, the UEI has automatically been assigned and no action is necessary. For all entities filing a new registration in SAM.gov on or after April 4, 2022, the UEI will be assigned to that entity as part of the SAM.gov registration process.

UEI registration information is available on GSA.gov at Unique Entity Identifier Update | GSA.

Visit Grants.gov for registration information. Detailed information regarding UEI and SAM is also provided in Section D of this funding notice.

Table of Contents

A. Program Description

1. Issued By
2. Assistance Listings Number
3. Assistance Listings Title

4. Funding Opportunity Title
5. Funding Opportunity Number
6. Authorizing Authority for Program
7. Appropriation Authority for Program
8. Announcement Type
9. Program Category
10. Program Overview, Objectives and Priorities
11. Performance Measures

B. Federal Award Information

1. Available Funding for the NOFO: $185 million
2. Projected Number of Awards: 56
3. Period of Performance: 48 months
4. Projected Period of Performance Start Date(s): Sept. 1, 2022
5. Projected Period of Performance End Date(s): Aug. 31, 2026
6. Funding Instrument Type: Grant

C. Eligibility Information

1. Eligible Applicants
2. Applicant Eligibility Criteria
3. Other Eligibility Criteria
4. Cost Share or Match

D. Application and Submission Information

1. Key Dates and Times
2. Agreeing to Terms and Conditions of the Award
3. Address to Request Application Package
4. Steps Required to Obtain a Unique Entity Identifier, Register in the System for Award Management (SAM), and Submit an Application
5. Electronic Delivery
6. How to Register to Apply through Grants.gov
7. How to Submit an Initial Application to FEMA via Grants.gov
8. Submitting the Final Application in ND Grants
9. Timely Receipt Requirements and Proof of Timely Submission
10. Content and Form of Application Submission

11. Intergovernmental Review
12. Funding Restrictions and Allowable Cost

E. Application Review Information

1. Application Evaluation Criteria
2. Review and Selection Process

F. Federal Award Administration Information

1. Notice of Award
2. Pass-Through Requirements
3. Administrative and National Policy Requirements
4. Reporting
5. Program Evaluation
6. Monitoring and Oversight

G. DHS Awarding Agency Contact Information

1. Contact and Resource Information
2. Systems Information

H. Additional Information

1. Termination Provisions
2. Period of Performance Extensions
3. Disability Integration
4. Conflicts of Interest in the Administration of Federal Awards or Subawards
5. Procurement Integrity
6. Record Retention
7. Actions to Address Noncompliance
8. Audits
9. Payment Information
10. Whole Community Preparedness
11. Continuity Capability
12. Appendices
    1. Appendix A: Goals and Objectives
    2. Appendix B: Planning Committee

3. Appendix C: Cybersecurity Plan
4. Appendix D: Multi-Entity Grants
5. Appendix E: Imminent Cybersecurity Threat
6. Appendix F: Investment Justification Form and Instructions
7. Appendix G: Required, Encouraged, and Optional Services, Memberships, and Resources
8. Appendix H: Economic Hardship Cost Share Waiver

A. Program Description

1. Issued By

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

2. Assistance Listings Number

97.137

3. Assistance Listings Title

State and Local Cybersecurity Grant Program (SLCGP)

4. Funding Opportunity Title

Fiscal Year 2022 State and Local Cybersecurity Grant Program (SLCGP)

5. Funding Opportunity Number

DHS-22-137-000-01

6. Authorizing Authority for Program

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

7. Appropriation Authority for Program

Infrastructure Investments and Jobs Appropriations Act (Pub. L. No. 117-58)

8. Announcement Type

Initial

9. Program Category

Preparedness: Community 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.

The potential consequences of cyber incidents threaten national security. Strengthening 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 Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their community.

The FY 2022 SLCGP aligns with the 2020-2024 DHS Strategic Plan by helping DHS achieve Goal 3: Secure Cyberspace and Critical Infrastructure, Objective 3.3. Assess and Counter Evolving Cybersecurity Risks. The FY 2022 SLCGP also supports the 2022-2026 FEMA Strategic Plan which outlines a bold vision and three ambitious goals, including Goal 3: Promote and Sustain a Ready FEMA and Prepared Nation, Objective 3.2: Posture FEMA to meet current and emergent threats.

b. Objectives

The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk. For Fiscal Year (FY) 2022, applicants are required to address how the following program objectives will be met in their applications:

- Objective 1: Develop and establish appropriate governance structures, including 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.

For more information on the program goals, objectives, sub-objectives, and desired outcomes, please refer to Appendix A.

c. Priorities

The Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law requires grant recipients to develop a Cybersecurity Plan, establish a Cybersecurity Planning Committee to support development of the Plan, and identify projects to implement utilizing SLCGP funding. To support these efforts, recipients are highly encouraged to prioritize the following activities using FY 2022 SLCGP funds, all of which are statutorily required as a condition of receiving a grant:

- Establish a Cybersecurity Planning Committee;
- Develop a state-wide Cybersecurity Plan, unless the recipient already has a state-wide Cybersecurity Plan and uses the funds to implement or revise a state-wide Cybersecurity Plan;
- Conduct assessment and evaluations as the basis for individual projects throughout the life of the program; and
- Adopt key cybersecurity best practices.

Cybersecurity Planning Committee The Planning Committee is responsible for developing, implementing, and revising Cybersecurity Plans (including individual

projects); formally approving the Cybersecurity Plan (along with the chief information officer, chief information security officer or an equivalent official); and assisting with determination of effective funding priorities (i.e., work with entities within the eligible entity's jurisdiction to identify and prioritize individual projects). To support these responsibilities, the Planning Committee must include the following entities:

- The eligible entity (i.e., state or territory);
- County, city, and town representation (if the eligible entity is a state);
- Institutions of public education within the eligible entity's jurisdiction;
- Institutions of public health within the eligible entity's jurisdiction; and
- As appropriate, representatives from rural, suburban, and high-population jurisdictions.

For more information on the Cybersecurity Planning Committee responsibilities and composition, please refer to Appendix B.

Cybersecurity Plan To assist in developing the required Plan, a Cybersecurity Plan Checklist containing information on what must be included in the Plan has been developed for use by SLCGP recipients. Recipients are encouraged to incorporate, where applicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, SLT governments. For more information on the Cybersecurity Plan and Cybersecurity Plan Checklist, please refer to Appendix C.

Key Cybersecurity Best Practices To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, SLT governments must take decisive steps to modernize their approach to cybersecurity, adopting security best practices and advancing toward Zero Trust Architecture. The following strategic elements, therefore, are required to be included in Cybersecurity Plans and in 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); and
- Migration to the .gov internet domain.

As individual government entities increase their cybersecurity maturity, implementing more advanced best practices, such as endpoint detection and response capabilities, as well as conducting regular penetration testing, will be recommended.

11. Performance Measures

Each grant recipient is required to collect data to allow DHS to measure performance of the awarded grant in support of the SLCGP metrics, which will be described in each Cybersecurity Plan.

The statute requires that "not later than one year after the date on which an eligible entity receives a grant…for the purpose of implementing [its] Cybersecurity Plan…, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until one year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in:

- Implementing the Cybersecurity Plan;
- Reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a state, local governments within the jurisdiction of the eligible entity."

If an eligible entity does not have a Cybersecurity Plan in place and receives an award, then the statute requires that not later than one year after the date on which the eligible entity receives a grant, and annually thereafter until one year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to:

- Develop or revise a Cybersecurity Plan; or

- 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.

In order to measure performance, DHS may request information throughout the period of performance. In its final performance report submitted at closeout, the recipient must submit sufficient information to demonstrate it has met the performance goals as stated in its award. DHS will measure the recipient's performance of the grant by comparing the number of activities and projects needed and requested in its investment justification with the number of activities and projects acquired and delivered by the end of the period of performance using the following programmatic metrics:

- Percentage of entities with CISA approved state-wide Cybersecurity Plans
- Percentage of entities with statewide cybersecurity planning committees that meet the Homeland Security Act of 2002 and this SLCGP Notice of Funding Opportunity (NOFO) requirements
- Percentage of entities conducting annual table-top and full-scope exercises to test cybersecurity plans; Percent of the entities' SLCGP budget allocated to exercises; or Average dollar amount expended on exercise planning for entities
- Percentage of entities conducting an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement
- Percentage of entities performing phishing training; Percent of entities conducting awareness campaigns; Percent of entities providing role-based cybersecurity awareness training to employees
- Percentage of entities adopting the Workforce Framework for Cybersecurity (NICE Framework) as evidenced by established workforce development and training plans
- Percentage of entities with capabilities to analyze network traffic and activities related to potential threats
- Percentage of entities implementing multi-factor authentication (MFA) for all remote access and privileged accounts
- Percentage of entities with programs to anticipate and discontinue use of end of life software and hardware
- Percentage of entities prohibiting the use of known/fixed/default passwords and credentials

- Percentage of entities operating under the ".gov" internet domain
- Number of cybersecurity gaps or issues addressed annually by entities

B. Federal Award Information

1. Available Funding for the NOFO

$185 million

For FY 2022, DHS will award state and territorial funds based on baseline minimums and population as required by the Homeland Security Act of 2002, and described below.

Each state and territory will receive a baseline allocation using thresholds established in the Homeland Security Act of 2002. All 50 States, the District of Columbia, and the Commonwealth of Puerto Rico will receive a minimum of $2,000,000 each, equaling 1% of total funds appropriated to DHS in FY 2022. Each of the four territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands) will receive a minimum of $500,000, equaling 0.25% of the total funds appropriated to DHS in FY 2022. $90,500,000, 50% of the remaining amount will be apportioned based on the ratio that the population of each state or territory bears to the population of all states and territories. The remaining $90,500,000, equaling the other 50% of the remaining amount, will be apportioned based on the ratio that the population of each state that resides in rural areas bears to the population of all states that resides in rural areas.

FY 2022 SLCGP Allocations

State/Territory	FY 2022 SLCGP Allocation
Alabama	$3,848,596
Alaska	$2,245,130
Arizona	$3,336,349
Arkansas	$3,162,746

State/Territory	FY 2022 SLCGP Allocation
California	$7,981,997
Colorado	$3,234,143
Connecticut	$2,681,116
Delaware	$2,224,803
District of Columbia	$2,081,394
Florida	$5,889,464
Georgia	$4,877,389
Hawaii	$2,243,739
Idaho	$2,550,109
Illinois	$4,404,622
Indiana	$3,949,173
Iowa	$3,073,518
Kansas	$2,820,015
Kentucky	$3,659,521
Louisiana	$3,327,540
Maine	$2,666,932
Maryland	$3,214,008
Massachusetts	$3,173,589
Michigan	$4,777,219
Minnesota	$3,606,482

State/Territory	FY 2022 SLCGP Allocation
Mississippi	$3,274,355
Missouri	$3,841,132
Montana	$2,428,110
Nebraska	$2,555,930
Nevada	$2,488,375
New Hampshire	$2,499,170
New Jersey	$3,380,963
New Mexico	$2,540,767
New York	$5,813,554
North Carolina	$5,362,452
North Dakota	$2,287,118
Ohio	$4,980,243
Oklahoma	$3,294,613
Oregon	$2,988,975
Pennsylvania	$5,207,249
Rhode Island	$2,190,484
South Carolina	$3,661,568
South Dakota	$2,341,978
Tennessee	$4,244,182
Texas	$8,469,945

State/Territory	FY 2022 SLCGP Allocation
Utah	$2,619,397
Vermont	$2,310,302
Virginia	$4,292,938
Washington	$3,667,735
West Virginia	$2,764,988
Wisconsin	$3,795,634
Wyoming	$2,200,558
Puerto Rico	$2,492,381
U.S. Virgin Islands	$500,000
American Samoa	$500,000
Guam	$500,000
Northern Mariana Islands	$500,000
Total	**$185,024,690**

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. FEMA awards under most programs, including this program, only include one budget period, so it will be same as the period of performance. See 2 C.F.R. § 200.1 for

definitions of “budget period” and “period of performance.”

4. Projected Period of Performance Start Date(s)

Sept. 1, 2022

5. Projected Period of Performance End Date(s)

Aug. 31, 2026

6. Funding Instrument Type

Grant

C. Eligibility Information

1. Eligible Applicants

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. Accordingly, the Governor designated State Administrative Agency (SAA) is the only entity eligible to submit SLCGP applications to DHS/FEMA.

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. Additionally, $6 million in funding will be directly available to Tribal entities under the forthcoming Tribal Cybersecurity Grant Program, which DHS expects to publish the NOFO in the fall of 2022.

“State” is defined in 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 Commonwealth of the Northern Mariana Islands; “Local government” is defined in 6 U.S.C. § 101(13) as

- A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;
- An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and
- A rural community, unincorporated town or village, or other public entity.

“Tribal government” for purposes of being an eligible entity for the Tribal Cybersecurity Grant Program is defined in 6 U.S.C. § 665g(1)(12) as the recognized governing body of any Indian or Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent published list of Federally Recognized Tribes.

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

2. Applicant Eligibility Criteria

Applicants must be an eligible entity, meaning one of the 56 states and territories that are eligible for the program. One or more eligible entities may form a multi-entity group.

3. Other Eligibility Criteria

Cybersecurity Plan To be eligible for FY 2022 SLCGP funding, each eligible entity is required to submit a Cybersecurity Plan that aligns with the criteria detailed in Appendix C.

The only exception is if an eligible entity certifies to the Secretary that:

- The activities that will be supported by a grant are:
  - Integral to the development of the Cybersecurity Plan of the eligible entity; or
  - Necessary 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; and
- The eligible entity will submit to the Secretary a Cybersecurity Plan for review by September 30, 2023.

Note that for multi-entity groups, in order to be eligible for an award, all eligible entities within the multi-entity group must already have a Cybersecurity Plan in place; multi-entity groups are not eligible for awards to develop a Cybersecurity Plan. See 6 U.S.C. § 665g(f), (i)(3).

Cybersecurity Planning Committee To be eligible for FY 2022 SLCGP funding, each eligible entity is required to establish a Cybersecurity Planning Committee comprised of the members summarized in Appendix B.

4. Cost Share or Match

Eligible entities, if applying as a single applicant, must meet a 10% cost share requirement for the FY 2022 SLCGP. The recipient contribution can be cash (hard match) or third-party in-kind (soft match). Eligible applicants shall agree to make available non-federal funds to carry out an SLCGP award in an amount not less than 10% of activities under the award. For FY 2022, 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. Unless otherwise authorized by law, the non-federal cost share requirement cannot be matched with other federal funds. For example, if the federal award were at a 90% cost share and the total approved budget cost was

$100,000, then:

- Federal share is 90% of $100,000 = $90,000
- Recipient share is 10% of $100,000 = $10,000

However, with this example, if the total cost ended up being $120,000, the federal share would remain at $90,000 due to the statutory formula even if it means the federal share ends up being lower than 90%. Any cost overruns will not be matched by this grant program and will be incurred by the recipient. With this example, if the total cost ended up being $80,000, then the 90% federal share would decrease to $72,000, and the recipient cost share would be $8,000.

Additionally, by statute, the cost share applies to each individual activity funded by the grant award rather than just to the cumulative total. Recipients must ensure that each activity's cost share is met. DHS interprets "activity" to mean all items approved as part of a submitted "Project Worksheet."

For a multi-entity group project, a cost share or cost match is not required for the FY 2022 SLCGP. For more information about multi-entity group projects, please refer to Appendix D.

The Secretary of Homeland Security may waive or modify the non-federal share for an individual entity if the entity demonstrates economic hardship. Additional information about the eligibility criteria for a cost share waiver, as well as how to submit a request for a cost share waiver from DHS is included in Appendix H.

D. Application and Submission Information

1. Key Dates and Times

a. Application Start Date:

Sept. 16, 2022

b. Application Submission Deadline:

Nov. 15, 2022 at 5 p.m. ET

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

The Non-Disaster (ND) Grants System has a date stamp that indicates when an application is submitted. Applicants will receive an electronic message confirming receipt of their 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.

DHS will not review applications that are received after the deadline or consider these late applications for funding. DHS 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 DHS to make an award.

Applicants experiencing technical problems outside of their control must notify DHS as soon as possible and before the application deadline. Failure to timely notify DHS of the issue that prevented the timely filing of the application may preclude consideration of the award. “Timely notification” of DHS means 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 additional assistance using the ND Grants System, please contact the ND Grants Service Desk at (800) 865-4076 or NDGrants@fema.dhs.gov. The ND Grants Service Desk is available Monday through Friday, 9 a.m. – 6 p.m. ET. If applicants have programmatic or grants management questions or concerns, please contact the Centralized Scheduling and Information Desk (CSID) by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9 a.m. – 5 p.m. ET.

C. Anticipated Funding Selection Date:

No later than Nov. 30, 2022

D. Anticipated Award Date:

No later than Dec. 31, 2022

E. Other Key Dates

Event	Suggested Deadline for Completion
Obtaining an 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 in Grants.gov	Four weeks before actual submission deadline
Registering in ND Grants	One week before actual submission deadline
Starting application in Grants.gov	One weeks before actual submission deadline
Submitting the final application in ND Grants	By the 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

Initial applications are processed through the Grants.gov portal. Final applications are completed and submitted through FEMA's Non-Disaster Grants (ND Grants)

System. Application forms and instructions are available at Grants.gov. To access these materials, go to http://www.grants.gov, select “Applicants” then “Apply for Grants”. In order to obtain the application package, select “Download a Grant Application Package”. Enter the Assistance Listing (formerly CFDA) and/or the funding opportunity number located on the cover of the program’s NOFO, select “Download Package,” and then follow the prompts to download the application package. In addition, the following Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Notice and all relevant NOFO is (800) 462-7585.

4. 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 from SAM.gov 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. Create a Grants.gov account;
- f. Add a profile to a Grants.gov account;
- g. Establish an Authorized Organizational Representative (AOR) in Grants.gov;
- h. Register in ND Grants;
- i. Submit an initial application in Grants.gov;

- **j. Submit the final application in ND Grants, including electronically signing applicable forms; and**
- k. 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.

Specific instructions on how to apply for, update, or verify an UEI number or SAM registration or establish an AOR are included below in the steps for applying through Grants.gov.

Applicants are advised that DHS 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 DHS 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, DHS 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. § 25.110(c)(2)(iii), if an applicant is experiencing exigent circumstances that prevents it from receiving a UEI number, if applicable, and completing SAM registration prior to receiving a federal award, the applicant must notify FEMA as soon as possible by contacting askcsid@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 a UEI number, if applicable, and complete SAM registration within 30 days of the federal award date.

5. 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 initial applications through Grants.gov and a final application through ND Grants.

6. How to Register to Apply through Grants.gov

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 Grants.gov account to apply for grants.

Organizations must also have a Grants.gov account to apply for an award under this program. Creating a Grants.gov account can be completed online in minutes, but DUNS and SAM registrations may take several weeks. Therefore, an organization's registration should be done in sufficient time to ensure it does not impact the entity's ability to meet required application submission deadlines. Complete organization instructions can be found on Grants.gov here: https://www.grants.gov/web/grants/applicants/organization-registration.html.

If individual applicants are eligible to apply for this grant funding opportunity, refer to:

b. Obtain an UEI Number:

All entities applying for funding, including renewal funding, prior to April 4, 2022, 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.

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 organizations applying online through Grants.gov must register with SAM. Failure to register with SAM will prevent your organization from applying through Grants.gov. SAM registration must be renewed annually. For more detailed instructions for registering with SAM, refer to: https://www.grants.gov/web/grants/applicants/organization-registration/step-2-register-with-sam.html.

Note: As a new requirement 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, if applicable, 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 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) 606-8220.

f. Create a Grants.gov Account:

The next step in the registration process is to create an account with Grants.gov. If applicable, applicants must know their organization's DUNS number to complete this process.

For more information, follow the on-screen instructions or refer to: https://www.grants.gov/web/grants/applicants/registration.html.

See also Section D.8 in this NOFO, “Submitting the Final Application in ND Grants,” for instructions on how to register early in ND Grants.

g. Add a Profile to a Grants.gov Account:

A profile in Grants.gov corresponds to a single applicant organization the user represents (i.e., an applicant) or an individual applicant. If you work for or consult with multiple organizations and have a profile for each, you may log in to one Grants.gov account to access all of your grant applications. To add an organizational profile to your Grants.gov account, if applicable, enter the DUNS number for the organization in the UEI field while adding a profile.

For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/add-profile.html.

h. EBiz POC Authorized Profile Roles:

After you register with Grants.gov and create an Organization Applicant Profile, the organization applicant's request for Grants.gov roles and access are sent to the EBiz POC. The EBiz POC will then log in to Grants.gov and authorize the appropriate roles, which may include the Authorized Organization Representative (AOR) role, thereby giving you permission to complete and submit applications on behalf of the organization. You will be able to submit your application online any time after you have been assigned the AOR role.

For more detailed instructions about creating a profile on Grants.gov, refer to: https://www.grants.gov/web/grants/applicants/registration/authorize-roles.html.

i. Track Role Status:

To track your role request, refer to: https://www.grants.gov/web/grants/applicants/registration/track-role-status.html.

j. Electronic Signature:

When applications are submitted through Grants.gov, the name of the organization applicant with the AOR role that submitted the application is inserted

into the signature line of the application, serving as the electronic signature. The EBiz POC **must** authorize individuals who are able to make legally binding commitments on behalf of the organization as an AOR; this **step is often missed, and it is crucial for valid and timely submissions**.

7. How to Submit an Initial Application to FEMA via Grants.gov

Standard Form 424 (SF-424) is the initial application for this NOFO.

Grants.gov applicants can apply online using a workspace. A workspace is a shared, online environment where members of a grant team may simultaneously access and edit different web forms within an application. For each Notice of Funding Opportunity, you can create individual instances of a workspace. Applicants are encouraged to submit their initial applications in Grants.gov at least seven days before the application deadline.

In Grants.gov, applicants need to submit the following forms:

- SF-424, Application for Federal Assistance; and
- Grants.gov Lobbying Form, Certification Regarding Lobbying

Below is an overview of applying on Grants.gov. For access to complete instructions on how to apply for opportunities using Workspace, refer to: https://www.grants.gov/web/grants/applicants/workspace-overview.html

a. Create a Workspace:

Creating a workspace allows you to complete it online and route it through your organization for review before submitting.

b. Complete a Workspace:

Add participants to the workspace to work on the application together, complete all the required forms online or by downloading PDF versions, and check for errors before submission.

c. Adobe Reader:

If you decide not to apply by filling out webforms you can download individual PDF forms in Workspace so that they will appear similar to other Standard or DHS forms. The individual PDF forms can be downloaded and saved to your local device storage, network drive(s), or external drives, then accessed through Adobe Reader.

NOTE: Visit the Adobe Software Compatibility page on Grants.gov to download the appropriate version of the software at: https://www.grants.gov/web/grants/applicants/adobe-software-compatibility.html

d. Mandatory Fields in Forms:

In the forms, you will note fields marked with an asterisk and a different background color. These fields are mandatory fields that must be completed to successfully submit your application.

e. Complete SF-424 Fields First:

The forms are designed to fill in common required fields across other forms, such as the applicant name, address, and UEI number. To trigger this feature, an applicant must complete the SF-424 information first. Once it is completed, the information will transfer to the other forms.

f. Submit a Workspace:

An application may be submitted through workspace by clicking the “Sign and Submit” button on the Manage Workspace page, under the Forms tab. Grants.gov recommends submitting your application package at least 24-48 hours prior to the close date to provide you with time to correct any potential technical issues that may disrupt the application submission.

g. Track a Workspace:

After successfully submitting a workspace package, a Grants.gov Tracking Number (GRANTXXXXXXXX) is automatically assigned to the application. The number will be listed on the confirmation page that is generated after submission.

Using the tracking number, access the Track My Application page under the Applicants tab or the Details tab in the submitted workspace.

h. Additional Training and Applicant Support:

For additional training resources, including video tutorials, refer to: https://www.grants.gov/web/grants/applicants/applicant-training.html Grants.gov provides applicants 24/7 (except federal holidays) support via the toll-free number (800) 518-4726, email at support@grants.gov and the website at https://www.grants.gov/support.html. For questions related to the specific grant opportunity, contact the number listed in the application package of the grant you are applying for.

If you are experiencing difficulties with your submission, it is best to call the Grants.gov Support Center and get a ticket number. The Support Center ticket number will assist FEMA with tracking your issue and understanding background information on the issue.

8. Submitting the Final Application in ND Grants

After submitting the initial application in Grants.gov, eligible applicants will be notified by FEMA and asked to proceed with submitting their complete application package in ND Grants. Applicants can register early with ND Grants and are encouraged to begin their ND Grants registration at the time of this announcement or, at the latest, seven days before the application deadline. Early registration will allow applicants to have adequate time to start and complete their applications.

Applicants needing assistance registering for the ND Grants system should contact ndgrants@fema.dhs.gov or (800) 865-4076. For step-by-step directions on using the ND Grants system and other guides, please see https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system.

In ND Grants, 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) are auto generated in ND Grants, but applicants may access these forms in advance through the Forms tab under the SF-424 family on Grants.gov.

Applicants should review these forms before applying to ensure they have all the information required.

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

As application submission is a two-step process, the applicant with the AOR role who submitted the application in Grants.gov will receive an acknowledgement of receipt and a tracking number (GRANTXXXXXXXX) from Grants.gov with the successful transmission of its initial application. **This notification does not serve as proof of timely submission, as the application is not complete until it is submitted in ND Grants.** Applicants can also view the ND Grants Agency Tracking Number by accessing the Details tab in the submitted workspace section in Grants.gov, under the Agency Tracking Number column. Should the Agency Tracking Number not appear, the application has not yet migrated from Grants.gov into the ND Grants System. Please allow 24 hours for your ND Grants application tracking number to migrate.

All applications must be received in ND Grants by **5 p.m. ET** on the application deadline. Proof of timely submission is automatically recorded by ND Grants. An electronic date/time stamp is generated within the system when the application is successfully received by ND Grants. Additionally, the applicant(s) listed as contacts on the application will receive a system-generated email to confirm receipt.

10. Content and Form of Application Submission

a. Standard Required Application Forms and Information

The following forms or information are required to be submitted in either Grants.gov or ND Grants. The Standard Forms (SF) are submitted either through Grants.gov, through forms generated in ND Grants, or as an attachment in ND Grants. Applicants may also access the SFs at https://www.grants.gov/web/grants/forms/sf-424-family.html.

i. Grants.Gov

- **SF-424, Application for Federal Assistance**, initial application submitted through Grants.gov
- **Grants.gov Lobbying Form, Certification Regarding Lobbying**, submitted through Grants.gov

ii. ND Grants

- **SF-424A, Budget Information (Non-Construction)**, submitted via the forms generated by ND Grants
- **SF-424B, Standard Assurances (Non-Construction)**, submitted via the forms generated by ND Grants
- **SF-LLL, Disclosure of Lobbying Activities**, submitted via the forms generated by ND Grants
- **Indirect Cost Agreement or Proposal**, submitted as an attachment in ND Grants if the budget includes indirect costs and the applicant is required to have an indirect cost rate agreement or proposal. If the applicant does not have or is not required to have an indirect cost rate agreement or proposal, please see Section D.13 of this NOFO, "Funding Restrictions and Allowable Costs," for further information regarding allowability of indirect costs and whether alternatives to an indirect cost rate agreement or proposal might be available, or contact the relevant FEMA staff identified in Section G of this NOFO, "DHS Awarding Agency Contact Information" for further instructions.

b. Program-Specific Required Forms and Information

The following program-specific forms or information are required to be submitted in ND Grants as file attachments:

- **SLCGP Investment Justifications:** Each eligible entity is required to submit complete project-level information detailing how the program objectives and goals will be met to develop, implement, or revise its Cybersecurity Plan; establish a Cybersecurity Planning Committee; conduct assessments and evaluations; and adopt key cybersecurity best practices. For more information on the Investment Justification, please refer to Appendix F. The FY 2022 Investment Justification must include the following information:

    - Only one application will be submitted by the eligible entity. It must include a brief description of the capabilities of the SLT agencies across the eligible entity related to the required elements of the Cybersecurity Plan.
    - The application will consist of up to four investments, one for each SLCGP objective (See Appendix F for more information on the goal and objectives).
    - Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP; however, it is important to note that identifying and mitigating gaps in the cybersecurity workforce, enhancing recruitment and retention efforts, and bolstering the knowledge, skills, and abilities of personnel are still statutory requirements for Cybersecurity Plans to address even if the eligible entity does not use grant funds to carry this out.
    - Requests to use funding to address imminent cybersecurity threats must be addressed in the Investment Justification (IJ) for Objective 3.
    - Each investment must describe how each project aligns to the entity's Cybersecurity Plan if applying for a grant to implement or revise the Cybersecurity Plan, or will align with the entity's Cybersecurity Plan if applying for a grant to develop a Cybersecurity Plan. Applicants must also describe how implementing the plan will be measured (metrics).
    - Each project must include an explanation of how the proposed project(s) will achieve the program objectives as identified in Appendix C. A project schedule with clearly defined milestones must also be included.
- **Cybersecurity Plan:** Each eligible entity is required to submit its Cybersecurity Plan that adheres to the 16 required elements identified in section 2220A of the Homeland Security Act of 2002 as amended by the BIL and included in Appendix C of this NOFO unless the eligible entity is applying for funds to develop a Cybersecurity Plan as described more below. The Cybersecurity Plan must include a description of SLT roles, an assessment of capabilities for each element, address resources and timeline for implementing the Plan, and identify metrics. SLT governments are encouraged to take a holistic approach in the development of their Plan as entities must be able to sustain capabilities once SLCGP funds are no longer available. The role of state entities as coordinator and service provider to local entities should be encouraged and supported. For more information on the Cybersecurity Plan, please refer to Appendix C.
- **Cybersecurity Planning Committee Membership List:** The Cybersecurity Planning Committee should be seen as a platform to identify and then prioritize

state-wide efforts, to include identifying opportunities to consolidate projects to increase efficiencies. Each eligible entity is required to submit confirmation that the committee is comprised of the required representatives. The eligible entity must also confirm that at least one-half of the representatives of the committee have professional experience relating to cybersecurity or information technology. For more information on the composition of the Cybersecurity Planning Committee, including how to leverage existing planning committees, please refer to Appendix B.

- **Cybersecurity Planning Committee Charter:** The Cybersecurity Planning Committee Charter must be submitted with the Cybersecurity Planning Committee Membership List attached as specified in Appendix B.
- **Cybersecurity Plan Submission Exception Request** (if applicable)
  - Applicants may request an exception to submitting their Cybersecurity Plan at the time of application. The exception request must be supported by the Chief Information Officer (CIO), Chief Information Security Office (CISO), or equivalent official.
  - If an exception is requested, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or are necessary to assist with activities that address imminent cybersecurity threats. Activities integral to the development of a Cybersecurity Plan are limited to investments and projects aligned to Objective 1 and Objective 2. Activities to address imminent cybersecurity threats are limited to investments and projects aligned to Objective 3.
  - **The eligible entity must also include a certification**, either as a separate document or as part of the applicable IJ(s), that all activities funded by the grant are integral to the development of the Cybersecurity Plan or are necessary 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. If grant funding is necessary to assist with activities that address imminent cybersecurity threats, then that should be noted on the applicable IJ.
  - Recipients seeking funding to develop a Cybersecurity Plan must still submit IJs for Objectives 1, 2, and 3, noting that they will need to be updated once the Cybersecurity Plan is completed and approved. It is still optional to submit an IJ for Objective 4.

- Once the Cybersecurity Plan is completed and approved by the Cybersecurity Planning Committee and CIO, CISO, or equivalent official, the applicant must then submit updated IJs for Objectives 1, 2, and 3, along with an updated IJ for Objective 4 if one was previously submitted, to DHS with the approved Cybersecurity Plan by September 30, 2023.

The following is required to request an exception:

- Statement from the applicant as to why they do not have an approved Cybersecurity Plan;
- High-level plan, including dates and milestones, for completing and submitting the Plan to DHS; and
- Signatures of support from the eligible entity and CIO, CISO, or equivalent official.

11. 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; https://www.whitehouse.gov/wp-content/uploads/2020/04/SPOC-4-13-20.pdf).

12. Funding Restrictions and Allowable Costs

All costs charged to awards covered by this NOFO must 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 award. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. See 2 C.F.R. § 200.403(h) (referring to budget periods, which for DHS awards under this program is the same as the period of performance).

In general, the Cost Principles establish standards for the allowability of costs, provide detailed guidance on the cost accounting treatment of costs as direct or administrative costs, and set forth allowability principles for selected items of cost. More specifically, except as otherwise stated in this NOFO, the terms and

condition of an award, or other program materials, costs charged to awards covered by this NOFO must be consistent with the Cost Principles for Federal Awards located at 2 C.F.R. Part 200, Subpart E. In order to be allowable, all costs charged to a DHS award or applied to the cost share must be reasonable in nature and amount and allocable to the particular DHS award.

Additionally, all costs charged to awards must comply with the grant program's applicable statutes, policies, requirements in this NOFO as well as with the terms and conditions of the award. If DHS staff identify costs that are inconsistent with any of these requirements, these costs may be disallowed, and DHS may recover funds as appropriate, consistent with applicable laws, regulations, and policies.

As part of these requirements, grant recipients and subrecipients may only use federal funds or funds applied to a cost share for the purposes set forth in this NOFO and the terms and conditions of the award, and those costs must be consistent with the statutory authority for the award.

Grant funds may not be used for matching funds for other federal grants/cooperative agreements, lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the federal government or any other government entity.

Specific investments made in support of the funding priorities discussed in this NOFO generally fall into one of the following seven allowable expense categories:

- Planning;
- Equipment;
- Exercises;
- Management & Administration (M&A);
- Organization; and
- Training.

In addition, any entity that receives FY 2022 SLCGP funding may not use the grant:

- 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;
- For any recipient cost-sharing contribution;
- To pay a ransom;
- For recreational or social purposes;
- To pay for cybersecurity insurance premiums;
- To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities; or
- 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.

a. Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services

Recipients and subrecipients of FEMA federal financial assistance are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200. Beginning August 13, 2020, the statute – as it applies to FEMA recipients, subrecipients, and their contractors and subcontractors – prohibits obligating or expending federal award funds on certain telecommunications and video surveillance products and contracting with certain entities for national security reasons.

Guidance is available at Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services (Interim) FEMA Policy #405-143-1, or superseding document.

Additional guidance is available Contract Provisions Guide: Navigating Appendix II to Part 200 - Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

Effective August 13, 2020, FEMA recipients and subrecipients **may not** use any FEMA funds under open or new awards to:

1. 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;
2. 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
3. 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 impacted 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:

i. Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, (or any subsidiary or affiliate of such entities);

ii. 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);

iii. Telecommunications or video surveillance services provided by such entities or using such equipment; or

iv. 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. § 200.471.

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. To request pre-award costs, a written request must be included with the application, signed by the AOR of the entity. The letter must outline what the pre-award costs are for, including a detailed budget break-out of pre-award costs from the post-award costs, and a justification for approval.

c. Management and Administration (M&A) Costs

Management and administration (M&A) activities are allowable under this program. M&A activities are those directly relating to the management and administration of SLCGP funds, such as financial management and monitoring. A maximum of up to five percent 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 five percent 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 five percent 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 or tribal jurisdictions must be based on the state's total SLCGP award prior to withholding any M&A.

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

Indirect costs are allowable under this program as described in 2 C.F.R. Part 200, including 2 C.F.R. § 200.414. Applicants with a current negotiated indirect cost rate agreement that desire to charge indirect costs to an award must provide a copy of their negotiated indirect cost rate agreement at the time of application. Not all applicants are required to have a current negotiated indirect cost rate agreement. Applicants that are not required by 2 C.F.R. Part 200 to have a negotiated indirect cost rate agreement but are required by 2 C.F.R. Part 200 to develop an indirect cost rate proposal must provide a copy of their proposal at the time of application. Applicants who do not have a current negotiated indirect cost rate agreement (including a provisional rate) and wish to charge the de minimis rate must reach out to the FEMA Grants Management Specialist for further instructions. Applicants who wish to use a cost allocation plan in lieu of an indirect cost rate must also reach out to the FEMA Grants Management Specialist for further instructions. Post-award requests to charge indirect costs will be considered on a case-by-case basis and based upon the submission of an agreement or proposal as discussed above or based upon on the de minimis rate or cost allocation plan, as applicable.

E. 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 the categories of planning, organization, exercises, training, or equipment, aligned to closing capability gaps or sustaining capabilities.

I. 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.

II. Organization

Organization costs are allowable under this program. States must justify proposed expenditures of SLCGP funds to support organization activities within their IJ

submission. Organizational activities include:

- Program management;
- Development of whole community partnerships that support the 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 planning, organization, training, exercise, and equipment 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.

III. 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, state and local governments.

Unless otherwise stated, all equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase using these funds. Please refer to FEMA's Authorized Equipment List. In addition, 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.

IV. 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 Cybersecurity Plan and 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 that may be more impacted by disasters, including 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, should be identified in an 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 (ADDIE) model of instructional design.

Recipients are also encouraged to utilize 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, territorial, and tribal audiences. The catalog can be accessed at http://www.firstrespondertraining.gov.

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.

V. 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 training requirements and EHP review can be found online at https://www.fema.gov/media-library/assets/documents/90195.

E. Application Review Information

1. Application Evaluation Criteria

a. Programmatic Criteria

DHS/FEMA will evaluate the FY 2022 SLCGP applications for completeness and applicant eligibility. DHS/CISA will evaluate the FY 2022 SLCGP applications for adherence to programmatic guidelines, and anticipated effectiveness of the proposed investments. The review will include verification of the following elements:

- Establishment of and composition of the Planning Committee;
- Cybersecurity Plan(s) or request for exception; and
- Proposed projects that are consistent with the Cybersecurity Plan(s), or will be consistent with the Cybersecurity Plan if requesting a grant to develop a Plan, and SLCGP program objectives and requirements.

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. DHS will use the information provided in the application and after the submission of the first Program Performance Report (PPR) to determine the feasibility and effectiveness of a grant project.

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 governmentwide eligibility qualification or financial integrity information, including whether the applicant is suspended or debarred. 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:

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

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:

1. FEMA is required 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).
2. An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.
3. 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 BIL 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. The federal review for compliance will be conducted by FEMA. 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. DHS will review IJs at both the investment and project level. The following criteria will be applied to the review of projects:

- Clarity: Sufficient detail to understand what the project is intending to do with grant dollars. (Yes/No)
- Logical/Project Alignment: Alignment with the stated SLCGP objectives and the applicant's Cybersecurity Plan or with the development of a Cybersecurity Plan. (Yes/No)
- Reasonableness: Costs for the items/services outlined within the project description are reasonable. Execution within the period of performance is feasible. (Yes/No)

Projects rated as effective or promising are approved. If an exception request from the FY 2022 Cybersecurity Plan submission requirement was submitted, SLCGP funds can only initially be used for activities that are integral to the development of the Cybersecurity Plan or to assist with activities that address imminent cybersecurity threats. This is limited to investments and projects aligned to Objective 1 and Objective 2.

In addition, investments with emergency communications activities will be reviewed to verify compliance with SAFECOM Guidance. 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

Before accepting the award, the AOR and recipient should carefully read the award package. The award package includes instructions on administering the grant award and the terms and conditions associated with responsibilities under federal awards. **Recipients must accept all conditions in this NOFO as well as any specific terms and conditions in the Notice of Award to receive an award under this program.**

Notification of award approval is made through the ND Grants system through an automatic electronic mail to the recipient's authorized official listed in the initial application. The recipient should follow the directions in the notification to confirm acceptance of the award.

Recipients must accept their awards no later than 60 days from the award date. The recipient shall notify FEMA of its intent to accept and proceed with work under the award or provide a notice of intent to decline through the ND Grants system. For instructions on how to accept or decline an award in the ND Grants system, please see the ND Grants Grant Recipient User Guide, which is available at https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system along with other ND Grants materials.

Funds will remain on hold until the recipient accepts the award through the ND Grants system and all other conditions of the award have been satisfied or until the award is otherwise rescinded. Failure to accept a grant award within the 60-day timeframe may result in a loss of funds.

2. Pass-Through Requirements

a. Generally

The eligible entity or multi-entity group must pass through at least 80 percent of the federal funds provided under the grant to local governments, including rural areas, within the jurisdiction of the eligible entity or multi-entity group.

Four requirements must be met to pass-through grant funds:

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

The signatory authority of the eligible entity must certify in writing to DHS/FEMA that pass-through requirements have been met. A letter of intent (or equivalent) to distribute funds is not considered sufficient; after the funds have been distributed, the SAA must self-certify, on behalf of the state, that the pass-through requirements have been met.

b. Rural Area Pass-Through

As part of the local government pass through requirement, in obligating funds, items, services, capabilities, or activities to local governments, each eligible entity or multi-entity group is required to pass through at least 25% of the federal funds provided under the grant to rural areas. Per the Homeland Security Act of 2002, a rural area is defined in 49 U.S.C. § 5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an “urbanized area” by the Secretary of Commerce.

The eligible entity or multi-entity group may either pass through 25% of the federal funds provided under the grant; items, services, capabilities, or activities having a 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 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 or multi-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 in order to count that value as part of the overall 80% pass-through 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

The local government pass-through requirement, including the rural area pass-through requirement, does not apply to:

- Grants awarded solely to support activities integral to the development or revision of the Cybersecurity Plan of the eligible entity; or
- The District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

D. Timing

The eligible entity must pass-through at least 80% of the funds awarded under the SLCGP to local governments, including at least 25% to rural areas, within 45 calendar days of receipt of the funds. “Receipt of the funds” occurs either when the eligible entity accepts the award or 15 calendar days after the eligible entity receives notice of the award, whichever is earlier.

Eligible entities are sent notification of SLCGP awards via the ND Grants system. If an eligible entity accepts its award within 15 calendar days of receiving notice of the award in the ND Grants system, the 45-calendar days pass-through period will start on the date the eligible entity accepted the award. Should an eligible entity not accept the SLCGP award within 15 calendar days of receiving notice of the award in the ND Grants system, the 45-calendar days pass-through period will begin 15 calendar days after the award notification is sent to the eligible entity via the ND Grants system.

It is important to note that the period of performance start date does not directly affect the start of the 45-calendar day pass-through period. For example, an eligible entity may receive notice of the SLCGP award on September 20, 2022, while the period of performance dates for that award are October 1, 2022, through September 30, 2025. In this example, the 45-day pass-through period will begin on the date the eligible entity accepts the SLCGP award or October 5, 2022 (15 calendar days after the eligible entity was notified of the award), whichever date occurs first. The period of performance start date of October 1, 2022 would not affect the timing of meeting the 45-calendar day pass-through requirement.

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

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

If a state 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 to gauge the level of interest in and obtain consent to receive these in lieu of funding. DHS also recommends including these councils or associations in the Cybersecurity Planning Committees. States should also inform local governments, including rural areas, that by signing up for state-wide items, services, capabilities, or activities, that they are providing consent to receive these in lieu of funding.

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 or rural area in lieu of funding. Consent can be given at individual local or tribal units of government, and does not have to be for all local governments within the state. If an individual unit of government does not consent to having the state retain a portion of funding, then the state must still pass-through funding to that local government, provided that entity has an approved project as part of the approved Cybersecurity Plan to utilize the funds.

In order for the SAA to retain more than 20% of SLCGP funds, the following conditions must be met:

- Must be for expenditures made by the state on behalf of the local or tribal government; and
- Must have written consent of the local or tribal government, specifying the amount of funds to be retained and the intended use of funds.

In providing these in lieu of funding, states must still ensure they are passing through an amount equal to at least 80% of the federal funding to local governments, including at least 25% to rural areas, within 45 days. The letter certifying the pass-through requirements have been met must indicate whether the state is passing through items, services, capabilities, or activities in lieu of funding as well as identify the consent it obtained from local governments. These decisions must also be documented in accordance with the Cybersecurity Planning Committee's Charter. For further information on Cybersecurity Planning Committee requirements, see Appendix B.

3. Administrative and National Policy Requirements

In addition to the requirements of in this section and in this NOFO, FEMA may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

a. DHS Standard Terms and Conditions

All successful applicants for DHS grant and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.

The applicable DHS Standard Terms and Conditions will be those in effect at the time the award was made. What terms and conditions will apply for the award will be clearly stated in the award package at the time of award.

B. Ensuring the Protection of Civil Rights

As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Recipients and subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at https://www.fema.gov/about/offices/equal-rights/civil-rights.

Monitoring and oversight requirements in connection with recipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7.

In accordance with civil rights laws and regulations, recipients and subrecipients must ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

C. Environmental Planning and Historic Preservation (EHP) Compliance

As a federal agency, FEMA is required to consider the effects of its actions on the environment and historic properties to ensure that all activities and programs funded by FEMA, including grant-funded projects, comply with federal EHP laws, Executive Orders, regulations, and policies, as applicable.

All non-critical new construction or substantial improvement of structures in a Special Flood Hazard Area must, at a minimum, apply the flood elevations of the Federal Flood Risk Management Standard's Freeboard Value Approach unless doing so would cause the project to be unable to meet applicable program cost-effectiveness requirements. All other types of projects may choose to apply the flood elevations of the Federal Flood Risk Management Standard's Freeboard Value Approach. See Executive Order (EO) 14030, Climate-Related Financial Risk and FEMA Policy #-206-21-0003, Partial Implementation of the Federal Flood Risk Management Standard for Hazard Mitigation Assistance Programs (Interim).

Recipients and subrecipients proposing projects that have the potential to impact the environment, including, but not limited to, the construction of communication towers, modification or renovation of existing buildings, structures, and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description along with any supporting documentation requested by FEMA in order to determine whether the proposed project has the potential to impact environmental resources or historic properties.

In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. Federal law requires EHP review to be completed before federal funds are released to carry out proposed projects. FEMA may not be able to fund projects that are not incompliance with applicable EHP laws, Executive Orders, regulations, and policies.

Executive Order (EO) 13985, Advancing Racial Equity and Support for Underserved Communities through the Federal Government, rearticulates and strengthens the environmental justice framework articulated in 1994 in EO 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations. Specifically, Section 1 of E.O. 13985 states that: "Affirmatively advancing equity, civil rights, racial justice, and equal opportunity is the responsibility of the whole of our Government. Because advancing equity requires a systemic approach to embedding fairness in decision-making processes, executive departments and agencies…must recognize and work to redress inequalities in their policies and programs that serve as barriers to equal opportunity."

Many projects funded by GPD's grant programs can have significant impacts on environmental justice. In particular, construction of buildings and other structures and construction of new communication towers may have disproportionately high and adverse effects on minority and low-income populations. FEMA acknowledges the important role that FEMA recipients and subrecipients play in advancing and achieving environmental justice by identifying low-income and minority populations within a proposed project's affected area as early as possible and taking steps to accommodate these interests.

For consistency with the Administration's policy, FEMA will review and evaluate potential projects for racial equity and justice concerns. If FEMA determines that a proposed project would have a disproportionately high and adverse effect on minority or low-income populations, FEMA will consult with recipients and subrecipients to discuss the feasibility of revising the scope of work to avoid these adverse impacts, or otherwise applying mitigation measures to alleviate these effects. In addition, FEMA may work with other recipients and subrecipients to solicit public input on the proposed projects for a more informed decision-making process. To learn more about how FEMA environmental justice responsibilities might affect your project, go to https://www.fema.gov/fact-sheet/executive-order-12898-environmental-justice.

DHS and FEMA EHP policy is found in directives and instructions available on the FEMA.gov EHP page, the FEMA website page that includes documents regarding EHP responsibilities and program requirements, including implementation of the National Environmental Policy Act and other EHP regulations and Executive Orders.

The GPD EHP screening form is located at https://www.fema.gov/media-library/assets/documents/90195. Additionally, all recipients under this funding opportunity are required to comply with the FEMA GPD EHP Policy Guidance, FEMA Policy #108-023-1, available at https://www.fema.gov/media-library/assets/documents/85376.

D. SAFECOM Guidance Compliance

All entities using SLCGP funding to support emergency communications investments are required to comply with the SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance). The SAFECOM Guidance provides current information on emergency communications policies, eligible costs, best practices, and technical standards for SLT recipients investing federal funds in emergency communications projects. It is also designed to promote and align with the National Emergency Communications Plan (NECP). Conformance with the SAFECOM Guidance helps ensure that federally funded investments are compatible, interoperable, resilient, and support national goals and objectives for improving emergency communications. Applicants should use the SAFECOM Guidance during planning, development, and implementation of emergency communications projects and in conjunction with other planning documents. Specifically, Appendix D of the SAFECOM Guidance contains compliance instructions for SLCGP grant recipients.

If an entity uses SLCGP funding to support emergency communications investments, the following requirements shall apply to all such grant-funded communications investments in support of the emergency communications priorities and recognized best practices: The signatory authority for the eligible entity must certify in writing to DHS/FEMA their compliance with the SAFECOM Guidance. The certification letter should be coordinated with the Statewide Interoperability Coordinator (SWIC) for each state and must be uploaded to ND Grants at the time of the first Program Performance Report (PPR) submission.

e. Requirement for using CISA Services

As a condition of receiving SLCGP funding, the grant recipient is required to adhere to or sign up for the following services, sponsored by CISA and further described in Appendix G, upon award as part of the statutory requirements in

developing, implementing, or revising a Cybersecurity Plan. Participation in these services and memberships are not required for submission and approval of a grant:

- Sign up for cyber hygiene services, specifically vulnerability scanning and web application scanning; and
- Complete the Nationwide Cybersecurity Review, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter.

Recipients and subrecipients are also encouraged to sign up for the other services and memberships identified in Appendix G.

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 on a quarterly basis through the FFR form (SF-425). Recipients may review the Federal Financial Reporting Form (FFR) (SF-425) at https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html#sortby=1

Recipients must file the FFR electronically using the Payment and Reporting Systems (PARS).

II. FFR REPORTING PERIODS AND DUE DATES

An FFR must be submitted quarterly throughout the period of performance, 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 period of performance. 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 period of performance for purposes of closeout, the following reporting periods and due dates apply for the FFR.

Reporting Period	Report Due Date
October 1 – December 31	January 30
January 1 – March 31	April 30
April 1 – June 30	July 30
July 1 – September 30	October 30

B. Programmatic Performance Reporting Requirements

I. PERFORMANCE PROGRESS REPORT (PPR)

Recipients are responsible for providing updated performance reports on an annual basis, consistent with the authorizing statute, as an attachment in ND Grants. The PPR should include a:

- Brief narrative of overall project(s) status;
- Summary of project expenditures;
- Description of any potential issues that may affect project completion; and
- Data collected for DHS performance measures.

Program Performance Reporting Periods and Due Dates The annual PPR submission is due January 30 of each year to account for the previous calendar year.

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 period of performance ends, recipients must liquidate all financial obligations and must submit the following:

1. The final request for payment, if applicable;
2. The final FFR (SF-425).).;
3. The final progress report detailing all accomplishments, including a narrative summary of the impact of those accomplishments throughout the period of performance; and
4. Other documents required by this NOFO, terms and conditions of the award, or other DHS/FEMA guidance.

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 deobligated, 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 FAPIIS 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:

1. Are presently excluded or disqualified;

2. 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;
3. 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
4. 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

Per 2 C.F.R. Part 200, Appendix I § F.3, the additional post-award reporting requirements in 2 C.F.R. Part 200, Appendix XII may apply to applicants who, if upon becoming recipients, have a total value of currently active grants, cooperative agreements, and procurement contracts from all federal awarding agencies that exceeds $10,000,000 for any period of time during the period of performance of an award under this funding opportunity.

Recipients that meet these criteria must maintain current information reported in FAPIIS 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

For audits of fiscal years beginning on or after December 26, 2014, recipients that expend $750,000 or more from all federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report, also known as the single audit report.

The audit must be performed in accordance with the requirements of U.S. Government Accountability Office's (GAO) Government Auditing Standards, located at https://www.gao.gov/yellowbook/overview, and the requirements of Subpart F of 2 C.F.R. Part 200, located at http://www.ecfr.gov/cgi-bin/text-idx?node=sp2.1.200.f.

5. Program Evaluation

Recipients and subrecipients are encouraged to incorporate program evaluation activities from the outset of their program design and implementation to meaningfully document and measure their progress towards the outcomes proposed. Title I of the Foundations for Evidence-Based Policymaking Act of 2018 (Evidence Act), Pub. L. No. 115-435 (2019) defines evaluation as "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). Credible program evaluation activities are implemented with relevance and utility, rigor, independence and objectivity, transparency, and ethics (OMB Circular A-11, Part 6 Section 290).

Evaluation costs are allowable costs (either as direct or indirect), unless prohibited by statute or regulation, and such costs may include the personnel and equipment needed for data infrastructure and expertise in data analysis, performance, and evaluation. (2 C.F.R. § 200).

In addition, recipients are required to participate in a DHS-led evaluation if selected, which may be carried out by a third-party on behalf of the Program Office or DHS. By accepting grant funds, recipients agree to participate in the evaluation, which may include analysis of individuals who benefit from the grant, and provide access to program operating personnel and participants, as specified by the evaluator(s) for six months after the period of performance.

6. Monitoring and Oversight

Per 2 C.F.R. § 200.337, DHS, through its authorized representatives, has the right, at all reasonable times, to make site visits or conduct desk reviews to review project accomplishments and management control systems to review award progress and to provide any required technical assistance, in the form of one-on-one guidance from a combination of Regional or Headquarters FEMA and CISA

Staff. During site visits or desk reviews, DHS will review recipients' files related to the award. As part of any monitoring and program evaluation activities, recipients must permit DHS, upon reasonable notice, to review grant-related records and to interview the organization's staff and contractors regarding the program. Recipients must respond in a timely and accurate manner to DHS requests for information relating to the award.

Effective monitoring and oversight help DHS 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. DHS regularly monitors 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. If the monitoring results in a determination that basic, minimum requirements as outlined in this NOFO are not being met, DHS may require corrective actions and/or initiate termination of the award.

DHS 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 DHS regulations. Aside from reviewing quarterly financial and annual programmatic reports, DHS 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 DHS's 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.

I. FINANCIAL MONITORING OVERVIEW AND APPROACH

FEMA's approach to financial 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:** 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.

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 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. Centralized Scheduling and Information Desk (CSID)

CSID is a non-emergency comprehensive management and information resource developed by FEMA for grants stakeholders. CSID 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. CSID can be reached by phone at (800) 368-6498 or by e-mail at askcsid@fema.dhs.gov, Monday through Friday, 9a.m. – 5 p.m. ET.

b. 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.

c. Equal Rights

The FEMA Office of Equal Rights (OER) in coordination with the DHS Office for Civil Rights and Civil Liberties 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.

D. 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. Grants.gov

For technical assistance with Grants.gov, call the customer support hotline 24 hours per day, 7 days per week (except federal holidays) at (800) 518-4726 or e-mail at support@grants.gov.

b. Non-Disaster (ND) Grants

For technical assistance with the ND Grants system, please contact the ND Grants Helpdesk at ndgrants@fema.dhsgov or (800) 865-4076, Monday through Friday, 9:00 AM – 6:00 PM ET. User resources are available at https://www.fema.gov/grants/guidance-tools/non-disaster-grants-management-system

c. Payment and Reporting System (PARS)

FEMA uses the Payment and Reporting System (PARS) for financial reporting, invoicing, and tracking payments. FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, recipients must complete a Standard Form 1199A, Direct Deposit Form. If you

have questions about the online system, please call the Customer Service Center at (866) 927-5646 or email ask-GMD@fema.dhs.gov.

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. Period of Performance Extensions

Extensions to the period of performance for this program are allowed. Extensions to the period of performance identified in the award will only be considered through formal, written requests to FEMA and must contain specific and compelling justifications as to why an extension is required. Recipients are advised to coordinate with FEMA and CISA, 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 period of performance 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 period of performance without any modification to the original statement of work, as described in the investment justification and as approved by DHS.

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 period of performance;
- The project must undergo a complex environmental review that cannot be completed within the existing period of performance;
- 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 DHS for review and approval at least 120 days prior to the end of the period of performance to allow sufficient processing time. Extensions are typically granted for no more than a six-month period.

3. 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 other qualified individuals with disabilities. Grant 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.

DHS 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 under this program:

- 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 to the extent practicable.
- Acquire language translation services, including American Sign Language, 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, language access, and information access. Examples of effective communication access include providing auxiliary aids and services such as sign language interpreters, Computer Aided Real-time Translation (CART), and materials in Braille or alternate formats.

FEMA grant recipients can fund projects towards the resilience 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.

4. 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 SLT 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 SLT 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 SLT statutes or regulations.

Conflicts of interest may arise during the process of DHS 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 DHS employees.

5. 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 SLT 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

OMB recently updated various parts of Title 2 of the Code of Federal Regulations, among them, the procurement standards. States are now 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 SLT 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/resources-for/programs-for-State-and-local-governments 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 FEMA Grants Management Specialist.

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.

6. 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
- 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.

7. 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, 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.

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 might 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 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 might 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; and
- Failure to comply with the POP deadline.

8. 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 whether 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 whether 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.

9. Payment Information

FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to recipients. To enroll in the DD/EFT, the recipient must complete SF-1199A, Direct Deposit Form.

FEMA utilizes the Payment and Reporting System (PARS) for financial reporting, invoicing and tracking payments. For additional information, refer to https://isource.fema.gov/sf269/execute/LogIn?sawContentMessage=true.

10. 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" or "Whole of Community" often appears in preparedness materials, as it is one of the guiding principles. It means:

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

11. 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/toolkit. For additional information on continuity programs, guidance, and directives, visit https://www.fema.gov/emergency-managers/national-preparedness/continuity.

This aligns with the requirements that 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).

12. Appendices

- Appendix A. Program Goals and Objectives
- Appendix B. Cybersecurity Planning Committee
- Appendix C. Cybersecurity Plan
- Appendix D. Multi-Entity Group Projects
- Appendix E. Imminent Cybersecurity Threats Process Overview
- Appendix F. Investment Justification Template and Instructions
- Appendix G. Required, Encouraged, and Optional Services, Memberships, and Resources
- Appendix H. Economic Hardship Cost Share Waiver

Appendix A: Goals and Objectives

Our nation faces unprecedented cybersecurity risk due to increasingly sophisticated adversaries, 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. In light of the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of SLT governments have become 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 working to achieve a cybersecurity ecosystem in which malicious actors face insurmountably high costs to execute damaging intrusions, vulnerabilities are rapidly identi?ed before exploitation, and technology is used to reduce the most harmful and systemic risks. 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 the Department 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 establish priorities the use of scarce resources and to develop metrics to gage 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 goals for the 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 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, as well as sample evidence of implementation are provided to assist the reader.

Goal of the State and Local Cybersecurity Grant Program: Assist SLT governments with managing and reducing systemic cyber risk.

Objective 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.

Sub-objective 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. Outcome: 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. Outcome: Participants have identified senior officials to enable whole-of-organization coordination on cybersecurity policies, processes, and procedures.

- Sample Evidence of Implementation: Organization has a cybersecurity defense concept of operations, with responsibilities assigned to specific organizational roles.

Sub-objective 1.2

Develop, implement, or revise, and test cybersecurity plans, including cyber incident response plans, with clearly defined roles and responsibilities.

1.2.1 Outcome: Develop, implement, or revise, and exercise cyber incident response plans.

- Sample Evidence of Implementation: Organization conducts annual table-top and full-scope exercises that include practical execution of restoration and recovery processes to test cybersecurity plans. Conducting these exercises allow organizations to test 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.

Sub-objective 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 Outcome: Ensure that systems and network functions are prioritized and reconstituted according to their impact to essential functions.

- Sample Evidence of Implementation: Organization conducts a regular business impact assessment to prioritize which systems must be protected and recovered first.

Objective 2

SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.

Sub-objective 2.1

Physical devices and systems, as well software platforms and applications, are inventoried. 2.1.1 Outcome: Establish and regularly update asset inventory.

- Sample Evidence of Implementation: Organization maintains and regularly updates an asset inventory list.

Sub-objective 2.2

Cybersecurity risk to the organization's operations and assets are understood.

2.2.1 Outcome: Conduct an annual cyber risk assessment to identify cyber risk management gaps and areas for improvement

- Sample Evidence of Implementation: Organization annually completes the Nationwide Cybersecurity Review (NCSR).

Sub-objective 2.3

Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.

2.3.1 Outcome: Participate in CISA's Vulnerability Scanning service, part of the Cyber Hygiene program.

- Sample Evidence of Implementation: Organization is an active participant in CISA's Cyber Hygiene program.

2.3.2 Outcome: Effectively manage vulnerabilities by prioritizing mitigation of high impact vulnerabilities and those most likely to be exploited.

- Sample Evidence of Implementation: 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.

Sub-objective 2.4

Capabilities are in place to monitor assets to identify cybersecurity events.

2.4.1 Outcome: 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.

Sub-objective 2.5

Processes are in place to action insights derived from deployed capabilities.

2.5.1 Outcome: SLT agencies are able to respond to identified events and incidents, document root cause, and share information with partners.

Objective 3

Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)

Sub-objective 3.1

SLT agencies adopt fundamental cybersecurity best practices.

3.1.1 Outcome: Implement multi-factor authentication (MFA), prioritizing privileged users, Internet-facing systems, and cloud accounts.

- Sample Evidence of Implementation: The organization implements MFA for all remote access and privileged accounts.

3.1.2. Outcome: End use of unsupported/end of life software and hardware that are accessible from the Internet.

- Sample Evidence of Implementation: The organization has a program to anticipate and discontinue use of end of life software and hardware.

3.1.3 Outcome: Prohibit use of known/fixed/default passwords and credentials.

- Sample Evidence of Implementation: The organization has a policy that prohibits fixed passwords, requires known/default passwords be immediately changed, and that passwords and credentials be periodically changed.
- Sample Evidence of Implementation: The organization has reviewed all of its current passwords and credentials to ensure they are updated appropriately.

3.1.4 Outcome: Ensure the ability to reconstitute systems following an incident with minimal disruption to services.

- Sample Evidence of Implementation: Organization policies require that backups for all critical systems and data be maintained, updated, and regularly tested according to organizational policy (e.g., quarterly), stored offline, and encrypted.

3.1.5 Outcome: Migrate to .gov internet domain.

- Sample Evidence of Implementation: Organization operates only the .gov internet domain, and does not use .com, .org, or any other domain.

Sub-Objective 3.2

Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.

3.2.1 Outcome: Individual participants address items identified through assessments and planning process.

3.2.2 Outcome: SLT entities improve cybersecurity ecosystem by collaborating to address items identified through assessments and planning process (e.g., regional and intra-state efforts)

Objective 4

Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Sub-Objective 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 Outcome: Organization requires regular ongoing phishing training, awareness campaigns are conducted, and organization provides role-based cybersecurity awareness training to all employees.

4.1.2 Outcome: Organization has dedicated resources and funding available for its cybersecurity professionals to attend technical trainings and conferences.

Sub-Objective 4.2

Organization has adopted the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

4.2.1 Outcome: Organization has established cyber workforce development & training plans, based on the NICE Cybersecurity Workforce Framework.

Appendix B: Planning Committee

Governance

In keeping with the guiding principles of governance for all Federal Emergency Management Agency (FEMA) preparedness programs and statutory requirements, recipients must coordinate activities across preparedness disciplines and levels of government, including SLT governments. A cohesive planning framework should incorporate FEMA resources, as well as those from other federal and SLT entities, the private sector, and faith-based community organizations. Specific attention should be paid to how available preparedness funding sources can effectively support a Whole Community approach to emergency preparedness and management and the enhancement of Core Capabilities. To ensure this, the State Administrative Agency (SAA) must establish or reestablish a unified 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)).

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 the 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 NOFO, and the

accompanying requirements, also apply to these alternative planning committee options.

Cybersecurity Planning Committee Composition and Scope Requirements

Cybersecurity Planning Committee membership shall include at least one representative from relevant stakeholders including:

- The eligible entity;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or equivalent official of the eligible entity;
- If the eligible entity is a state (including territories), then 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 Cybersecurity Planning Committee must have professional experience relating to cybersecurity or information technology. Qualifications are determined by the states.

Eligible entities are given the flexibility to identify the specific public health and public education agencies and communities these members represent. DHS strongly encourages eligible entities to consider naming additional members to the Cybersecurity Planning Committee, including but not limited to representatives from:

- State and county judicial entities;
- The Chief Information Officer (CIO), the Chief Information Security Officer (CISO, or equivalent official of the eligible entity;
- 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 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. The Cybersecurity Planning Committee POC's contact information must be provided to FEMA as part of the grant application. Eligible entities must ensure that information for current points of contact is on file with FEMA.

Eligible entities must submit the list of Cybersecurity Planning Committee members at the time of application as an attachment in ND Grants. Eligible entities must verify compliance with Cybersecurity Planning Committee charter requirements. The below table provides a suggested format for submitting the list of required Cybersecurity Planning Committee members.

Representation	Name	Title	Organization	Cybersecurity/IT Experience (Yes/No)
Eligible entity				
If eligible entity is a state, counties, cities, and towns within the jurisdiction of the entity				
Institution of Public Education within the eligible entity				

Representation	Name	Title	Organization	Cybersecurity/IT Experience (Yes/No)
Institution of Public Health within the eligible entity				
(Additional)				
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 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 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.

Local Consent

Eligible entities or multi-entity groups are statutorily required to provide at least 80% of the federal funding to local governments, including at least 25% rural areas. With the consent of the local governments, part or all of this pass-through can be in the form of items, services, capabilities, or activities. This flexibility in the type of funds that are passed through may assist eligible entities or multi-entity groups in promoting projects that have state-wide (or broader) impacts, and they may be able to more effectively reduce cybersecurity risk if managed at the state or multi-state level. Examples of these types of projects include the purchase of software licenses or development of capabilities. Any decision to pass through some or all of the funds via items, services, capabilities, or activities must be explicitly consented to by the local governments and must be documented in accordance with the Cybersecurity Planning Committee's Charter and comply with Section F.2 of this NOFO for further information.

Cybersecurity Planning Committee Charter

The governance of the SLCGP through the Cybersecurity Planning Committee should be directed by 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 must submit the Cybersecurity Planning Committee charter at the time of application as an attachment in ND Grants. Revisions to the governing charter must also be sent to the recipient's assigned FEMA HQ 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 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 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 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

Cybersecurity Plan Basics

- Comprehensive strategic plan to reduce cybersecurity risk and increase capability across the entity
- Entity-wide plan, not a single entity

- Should cover 2 to 3 years
- Must include required elements, with discretion to add other elements as necessary
- Existing plans can be utilized
- There is no required template, but required elements must be identifiable for review purpose
- Individual projects must align to Cybersecurity Plan
- Must be approved by the Cybersecurity Committee **and** CIO/CISO/Equivalent
- CISA approves for DHS
- Plans are initially approved for 2 years; annually thereafter

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

Accordingly, 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.

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

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

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 overall plan requirements and additional considerations that eligible entities should consider when constructing the Cybersecurity Plan. Although there is no required format for the Cybersecurity Plan, 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 downstream 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 below). 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. While 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.
- 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 map how the 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. It should also map 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 Investment Justification.
- 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-A.11 and Appendix A of this NOFO. Additional information is provided in the Cybersecurity Plan Metric Section below and also in the Cybersecurity Plan Template.

- Approvals - the Cybersecurity Plan must be approved by the Cybersecurity Planning Committee and the CIO/CISO/Equivalent. 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.

Cybersecurity Planning Committees should also consider the following when constructing 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 projects should demonstrably support the state, territorial, and local entities in achieving those capabilities over time.
- Focused investments that are sustainable over time. The SLCGP currently is authorized for four years and limited funds are available. Cybersecurity Plans must address how SLT entities will sustain capabilities once the program ends or funds are no longer available.
- State role as leader and service provider. Many states 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 (See Appendix D for additional information on multi-entity activities).
- 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 Cybersecurity Planning Committee.

Required Cybersecurity Best Practices

Although these cybersecurity best practices must be addressed in the Cybersecurity Plan, 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. Individual projects that assist SLT entities adopt these best practices should also be prioritized by the Cybersecurity Planning Committee. As there are multiple ways to implement the best practices, this approach 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 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 description 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); and
- Migration to the .gov internet domain.

Additional best practices that the Cybersecurity Plan can address include:

- The National Institute of Standards and Technology (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 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 G 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 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 jurisdiction. The assessment will become the road map for individual projects and activities using SLCGP funds. All Investment Justifications must reference the capability gaps identified in the assessment. The Cybersecurity Plan Capabilities Assessment Worksheet (see Cybersecurity Plan Template) provides an easy way for 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 implement the plan over time. A summary of projects using FY 2022 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 Investment Justification (see Appendix F) and is 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)]

Graphic

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

Cybersecurity Plan Metrics

Cybersecurity Plans must include language detailing how the state will measure both: 1) how the state will implement the plan; and 2) how the state will reduce cybersecurity risks to, and 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. See page 6 of this NOFO for additional information on required metrics and reporting.

States, and their Cybersecurity Planning Committees in helping with Cybersecurity Plans, should consider the following when developing metrics:

- Aligning metrics to the Cybersecurity Plan and the established program goals and objectives included at Appendix A.
- Reviewing existing metrics that are in use across the state; and
- The data for each metric must be available and reportable and should not create unnecessary burdens to collect.

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

Graphic

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		
3.	3.1		
	3.2		
4.	4.1		
	4.2		
	4.3		

Appendix D: Multi-Entity Grants

Multiple eligible entities can group together to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions that comprise the group. There is no separate funding for multi-entity awards. Instead, these investments would be considered as group projects and be funded out of the participating entities' published allocations. These projects should be included as individual Investment Justifications from each participating eligible entity, each approved by the respective Cybersecurity Planning Committee, and each aligned with the eligible entity's Cybersecurity Plan.

Eligibility

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

Cybersecurity Plan.

Additionally, note that for multi-entity groups, all individual eligible entities must have already developed a Cybersecurity Plan.

Benefits

Cost Savings: A multi-entity grant will be counted against the total apportionment of each entity. However, multi-entity grants may permit smaller entities to combine resources with larger entities to reap the benefits associated with larger acquisitions. At the same time, all parties to a multi-entity grant may realize cost savings due to volume purchases. The multi-entity group will also benefit from a total of 10% reduction in cost share requirements for that specific project. For FY 2022, this means that multi-entity projects would not require any recipient cost share.

Shared Resources: Since the multi-entity group may be comprised of state (including territorial) governments, each shall benefit from information sharing and awareness opportunities.

Requirements and Process Overview

- Eligible entities work collaboratively to define the group project and the roles and responsibilities for each eligible entity.
- Each eligible entity must have a Cybersecurity Plan that has been approved by CISA – there is no exception to allow multi-entity groups to use a grant to develop any entity's Cybersecurity Plan.
- The project must improve or sustain capabilities identified in the respective Cybersecurity Plans for each eligible entity.
- The Cybersecurity Planning Committee of each participating eligible entity must approve the individual project.
- Each eligible entity will be required to submit an Investment Justification describing the following:
  - A description of the overarching multi-entity project;
  - The other eligible entities and all participating state, local, tribal, and territorial entities and identify the division of responsibilities amongst the multi-entity group;

- The distribution of funding from the grant among the eligible entities that comprise the multi-entity group, to include any subawards made to local entities; and
- How the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

Additional details can be found in Appendix F – Investment Justification. Note: It is expected that Investment Justifications for multi-entity projects will be almost identical. Any differences should be as a result of alignment with the entities' respective Cybersecurity Plans.

Appendix E: 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 will reduce the potential impact of cybersecurity threats and incidents. The State and Local Cybersecurity Improvement Act enumerates, as one eligible use of funds, activities that address imminent cybersecurity threats, as follows: "An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate shall use the grant to…(4) 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." 6 U.S.C. § 665g(d)(4).

The following provides an overview of the processes for the FY 2022 grant cycle from a grant management perspective. Specific 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 seeking to use 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 unless DHS has granted the eligible entity an exception for the FY 2022 grant cycle to use the grant to develop a Cybersecurity Plan.
- Only DHS, through CISA, confirms an imminent cybersecurity threat.
- SLT entities cannot request a threat to be confirmed an imminent cybersecurity threat.
- Upon confirmation, DHS will notify the State Administrative Agency (SAA) at the eligible entity. DHS will notify impacted SLT entities as appropriate.
- FEMA will issue an Information Bulletin detailing the impacted entities and procedures for reprograming 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.
- The eligible entity must notify the Cybersecurity Planning Committee and chief information officer (CIO)/chief information security officer (CISO)/equivalent of the eligible entities, which are responsible for reviewing, prioritizing, and approving projects under SLCGP.
  - Impacted SLT entities should be notified consistent with established governance structures and notification processes within the eligible entity.
- It will be left at the discretion of eligible entity, in consultation with the Cybersecurity Planning Committee and CIO/CISO/equivalent, and in collaboration with other entities as necessary, to review the imminent cybersecurity threat information and determine if SLCGP funds are to be used to assist with activities that address the imminent cybersecurity threats.
- If the eligible entity wants to use any of its grant funds to address imminent cybersecurity threats that may arise during the period of performance, the eligible entity must include this in and submit an Investment Justification aligned to Objective 3. There is no minimum amount that the eligible entity must request or reserve through this Investment Justification, and if the eligible entity needs to reallocate funding across its approved Investment Justifications to address imminent cybersecurity threats, the eligible entity should collaborate with any subrecipient potentially impacted by the reallocation of funds.

Appendix F: Investment Justification Form and Instructions

Overview

Only one application will be submitted by the eligible entity. The application will consist of up to four (4) Investments, one for each SLCGP objective (see Appendix A for more information on the goal and objectives).

Investments for SLCGP Objectives 1, 2, and 3 must have at least one project. Investments for SLCGP Objective 4 are optional for the FY 2022 SLCGP. If an IJ is submitted for Objective 4, then it also must have at least one project.

For each objective, whether required or optional, Applicants must submit up to one IJ form per SLCGP objective, and at least one Project Worksheet for each submitted Investment Justification. Each IJ should have the same application-level information. Project level information should vary based on the associated SLCGP Objective.

Use the following naming convention for the IJs and Project Worksheets: [Insert name of state or territory] Objective [insert number of corresponding objective – 1, 2, 3 or 4]. For example: Alaska Objective 2.

Multi-entity efforts must be included as individual projects in the Project Worksheet, aligned to the appropriate investment (i.e., SLCGP objective). Additional information is provided below

General Process

- Download IJ Template.
- Download IJ Project Worksheet.
- Save a separate IJ Template and Project worksheet for each SLCGP Objective.
- Add the same portfolio information to each IJ file.
- Complete the investment level information for each objective.
- Identify individual projects for each objective using the Project Worksheet.
- Submit the following files via ND Grants:
  - Cybersecurity Plan (unless requesting an exemption)
  - One (1) IJ form for each SLCGP objective.
  - One (1) Project worksheet for each SLCGP objective.

Applicants should download the IJ Template at the link provided above to complete for each SLCGP objective. The IJ Template used for this program is from the approved collection for the Homeland Security Grant Program, but many

of the elements still apply to SLCGP. The instructions in the last column explain how a field in the IJ Template applies or does not apply to SLCGP. Please contact the applicable FEMA Preparedness Officer if unsure whether any elements of the IJ Template are required to be filled out.

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

All SLCGP recipients and subrecipients are required to participate in a limited number of free services by CISA. For these required services and memberships, please note that participation is not required for submission and approval of a grant but is a post-award requirement.

All SLCGP recipients are strongly encouraged to participate in other memberships.

Additional, optional CISA resources are also available in this Appendix

Required Services and Memberships

Cyber Hygiene Services

- Web Application Scanning is an “internet scanning-as-a-service.” This service assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
- Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@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 SLGCP.

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 National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC.

Entities and their subrecipients should 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 (NCSR) (cisecurity.org).

Encouraged Services, Membership and Resources

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 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).

The EI-ISAC, is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government

Coordinating Council. The EI-ISAC 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 the federal and SLT governments, as well as public and private sector critical infrastructure organizations:

- Ransomware Guide (Sept. 2020)
- Cyber Resilience Review
- External Dependencies Management Assessment
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Validated Architecture Design Review
- Free Public and Private Sector Cybersecurity Tools and Services

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 Standards Organization.

Appendix H: Economic Hardship Cost Share Waiver

The Homeland Security Act of 2002, as amended, requires SLCGP recipients in FY 2022 to provide a non-federal cost share of 10% if they are applying as a single entity (6 U.S.C. § 665g(m)(1)). For entities unable to meet the requirement, an economic hardship waiver may be granted by the DHS Secretary (or designee). 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.

Note that there is no cost share requirement for multi-entity groups for FY 2022. In addition, in accordance with 48 U.S.C. § 1469a, the Secretary has issued a blanket waiver of 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.

Economic Hardship Factors

Requests for cost share waivers may be granted by the Secretary (or designee) to an eligible entity that demonstrates economic hardship.

The statute, at 6 U.S.C. § 665g(m)(2)(C) requires the Secretary (or designee) to consider the following factors when determining economic hardship:

- Changes in rates of unemployment in the jurisdiction from previous years; and
- 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.

In addition, for FY 2022, the Secretary (or designee) will also consider the following factors in determining economic hardship:

- Demonstration of fiscal distress that could be caused by changes to statewide budgets already approved prior to knowledge of the SLCGP cost share requirement;
- Demonstration that the rate of unemployment has exceeded the annual national average rate of unemployment for three of the past five years;
- Demonstration that the entity has filed for bankruptcy or been placed under third-party financial oversight or receivership within the past three years; and
- For local units of government only, demonstration that those localities have areas within them that are designated as either “high” or “very high” on the Centers for Disease Control and Prevention’s Social Vulnerability Index.

To be considered for a cost share waiver, eligible entities must meet at least one of the six criteria 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.

Waiver Request Requirements

Eligible entities that would like to request an economic hardship waiver should submit a waiver request with its FY 2022 SLCGP application submission in ND Grants with the following information in a written narrative:

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

Approval Process

Once a decision on a waiver request is made, the state 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 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 or the Centralized Scheduling and Information Desk at askcsid@fema.dhs.gov or 1-800-368-6498.