NEW MEXICO DEPARTMENT OF HOMELAND SECURITY AND EMERGENCY MANAGEMENT

State and Local Cybersecurity Grant Program (SLCGP) 2022 Funding Announcement and Allocation Methodology

This page intentionally left blank

Table of Contents

This page intentionally left blank

State and Local Cybersecurity Grant Program (SLCGP) 2022
Funding Announcement and Allocation Methodology

A. PURPOSE

The State and Local Cybersecurity Grant Program (“SLCGP”) provides funding to state, local, and tribal entities to address cybersecurity risks and threats to entity-owned or operated information systems. This funding is made available through the Infrastructure Investment and Jobs Act, also known as the Bipartisan Infrastructure Law.

B. OBJECTIVES

The objective of the SLCGP is to make targeted cybersecurity investments to strengthen the cybersecurity practices and the resilience of state, local, and tribal governments.

C. PRIORITIES

The Homeland Security Act of 2002, as amended by the Bipartisan Infrastructure Law, requires grant recipients to develop a Cybersecurity Plan. The Cybersecurity Planning Committee of the New Mexico Office of Cybersecurity received U.S. Department of Homeland Security (DHS) approval of the New Mexico Cybersecurity Plan in September of 2023. The Cybersecurity Planning Committee prioritized utilization of FY 2022 SLCGP funding to support the following activities:

- Establish a Cybersecurity Planning Committee;
- Develop and maintain a statewide Cybersecurity Plan;
- Conduct assessments and evaluations as the basis for individual projects throughout the life of the program; and
- Adopt key cybersecurity best practices.

D. ELIGIBILITY CRITERIA

The New Mexico Department of Homeland Security and Emergency Management (“NMDHSEM”) in collaboration with the New Mexico Office of Cybersecurity and the Cybersecurity Planning Committee is offering local government entities in New Mexico (“Eligible Subrecipients”) the opportunity to participate in the SLCGP and receive State-provided services, direct funding, or both.

A “local government” entity is defined in 6 U.S.C. § 101(13) as:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

E. APPROVED SLCGP PROJECTS AND GRANT APPLICATION OPTIONS

Through the development of the New Mexico Cybersecurity Plan, the Cybersecurity Planning Committee has identified and approved five (5) FY 2022 SLCGP Projects to increase cybersecurity capabilities for Eligible Subrecipients (“the approved FY 2022 SLCGP Projects”).

1. Approved FY 2022 SLCGP Projects

(1) **Cybersecurity Governance and Planning** – Obtain assistance in establishing or enhancing cybersecurity governance (e.g., cyber plans, policies & procedures, standards, organization structure) to include receiving guidance and support with planning activities aimed at implementing or increasing the adoption of cyber-hygiene and best practices (e.g., multi-factor authentication, enhanced logging, migration to .gov internet domain).

(2) **Cybersecurity Risk Assessments** – Obtain assistance in performing cybersecurity risk

assessments utilizing the Nationwide Cybersecurity Review (NCSR), etc. to understand participating entities' cybersecurity posture and identify cybersecurity risks and control gaps, which will then be leveraged to update the New Mexico Cybersecurity Plan and for prioritizing future SLCGP-funded investment projects.

(3) **Vulnerability and Attack Surface Management** – Obtain services resulting from the deployment and integration of vulnerability and attack surface management capabilities for mitigating cybersecurity risks.

(4) **Cybersecurity Training** – Obtain basic cybersecurity awareness and phishing training for employees.

(5) **Cybersecurity Workforce Development Planning** – Participate in the development of a strategic plan and roadmap leveraging the Workforce Framework for Cybersecurity (NICE Framework) to assess cybersecurity workforce capabilities, as well as to plan for the implementation of cybersecurity workforce development and training programs based on the NICE Framework.

2. Grant Application Options

An Eligible Subrecipient has three participation options:

1. Participate as a recipient of State-provided services from the New Mexico Office of Cybersecurity;
2. Participate as a recipient of direct funding to independently implement projects; or
3. Participate as a recipient of services from the Office of Cybersecurity AND as a recipient of direct funding to independently implement projects.

Option 1: Participate as a recipient of State-provided services from the Office of Cybersecurity.
An Eligible Subrecipient may apply to participate as a subrecipient under the SLCGP and receive services from the Office of Cybersecurity to implement one or more of the approved FY 2022 SLCGP projects. There are no cost share or reporting requirements associated with an application to participate as a subrecipient under the SLCGP to receive services from the Office of Cybersecurity to implement one or more of the approved FY 2022 SLCGP Projects.

Eligible Subrecipients choosing this option will be responsible for:

1. Completing and submitting a signed FY 2022 SLCGP Local Consent Agreement with their application. This form is available for download using the following link: https://www.nmdhsem.org/wp-content/uploads/2024/02/New-Mexico-Local-Consent-Form_15Nov2023.pdf.
2. Participating in required CISA Cyber Hygiene Services.
3. (Optional) Completing the annual NCSR.

Option 2: Participate as a recipient of direct funding to independently implement projects.
An Eligible Subrecipient may apply for direct funding, as a subrecipient under the SLCGP, to independently implement one or more of the approved FY 2022 SLCGP projects. Additional information about the requirements and information for Option 2 can be found in *Appendix A: Direct Funding Requirements and Information*.

Entities choosing this option will be responsible for:

1. Completing the investment justification information included in the 'New Mexico FY 2022 SLCGP Subrecipient Grant Application: Opting Out of State-provided service(s)' webform
2. Completing and submitting an FY 2022 SLCGP Project Worksheet with their application. This form is available for download using the following link: https://www.nmdhsem.org/wp-content/uploads/2024/02/New-Mexico-FY-2022-SLCGP-Sub-Recipient-Project-Worksheet-template_15Dec2023.xlsx.
3. Meeting applicable cost share requirements for grant years 2 through 4.

4. All SLCGP requirements identified in *Appendix A: Direct Funding Requirements and Information* and the FY 2022 SLCGP NOFO.
   a. Participating in required CISA Cyber Hygiene Services;
   b. Completing the NCSR during the first year of the award/subaward period of performance and annually thereafter;
   c. Complying with funding restrictions outlined in the FY 2022 SLCGP NOFO:
      i. Restrictions on Covered Telecommunications Equipment or Services;
      ii. Allowable spending associated with planning, organization, equipment, training, exercise, Management and Administration (M&A), and Indirect Facilities and Administrative (F&A) costs;
      iii. DHS Standard Terms and Conditions; and
      iv. SAFECOM Guidance.
5. Completing and submitting all Quarterly Performance Reports (QPR) due to NMDSHEM by January 15th, April 15th, July 15th, and October 15th each year.
6. Completing and submitting all Quarterly Financial Reports (QFR) due to NMDSHEM by January 15th, April 15th, July 15th, and October 15th each year.

Option 3: Participate as a recipient of services from the Office of Cybersecurity AND as a recipient of direct funding to independently implement projects.

An Eligible Subrecipient may apply to participate as a subrecipient under the SLCGP to receive both State-provided services and direct funding to independently implement and manage projects. The requirements for both Option 1 and Option 2 will apply if an Eligible Subrecipient chooses this option. Additional information about the requirements and information for Option 3 can be found in *Appendix A: Direct Funding Requirements and Information*.

F. APPLICATION INSTRUCTIONS

All application-related documents for State-provided services and/or direct funding for local government-provided projects **MUST** be submitted no later than **April 30, 2024**. Late submissions will not be accepted.

I. State-Provided Services

1. Visit the NMDHSEM Grants website: https://www.nmdhsem.org/administrative-services-bureau/administrative-services-bureau-grants/
2. Click on the link for the State and Local Cybersecurity Grant Program (SLCGP).
3. Review:
   - FY 2022 SLCGP Funding Announcement and Allocation Methodology (this document)
   - New Mexico FY 2022 SLCGP Local Consent Agreement form
   - Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program included Appendix G
4. Click the link: 'CLICK HERE TO BEGIN YOUR APPLICATION'.
5. Click 'Submit' next to 'New Mexico FY 2022 SLCGP Subrecipient Grant Application: State-provided service(s)' and then follow the instructions, including to:
   - **Complete**, **sign**, and **submit** your New Mexico FY 2022 SLCGP State-provided service(s) subrecipient grant application.
   - **Complete**, **sign**, and **upload** the New Mexico FY 2022 SLCGP Local Consent Agreement. **This document MUST be included with your grant application if you are applying for one (1) or more projects as State-provided services.**

II. Direct Funding of Local Government Projects

A. Preparing for the Application Process:

1. **Unique Entity ID:** All applicants **MUST** include a Unique Entity ID (UEI) number when requested on application document(s). If your organization does not have a UEI number or if you need to verify your UEI number visit the SAM.GOV website at: https://sam.gov/content/entity-registration.
2. **Employer Identification Number:** All applicants **MUST** provide an Employer Identification Number (EIN) number when requested on application document(s). Your 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.
3. **New Mexico Statewide Human Resource, Accounting and Management Reporting System (SHARE) Vendor Number**: All applicants **MUST** provide a SHARE vendor number when requested on application document(s). Contact the NMDHSEM Grants Management Bureau for assistance in obtaining a SHARE number: dhsem-grantsmanagement@state.nm.us.

B. Completing the Application Process

1. Visit the NMDHSEM Grants website: https://www.nmdhsem.org/administrative-services-bureau/administrative-services-bureau-grants/.
2. Click on the link for the 2022 State and Local Cybersecurity Grant Program.
3. Review:
   - FY 2022 SLCGP Funding Announcement and Allocation Methodology (this document)
   - New Mexico FY 2022 SLCGP Project Worksheet form
   - Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program included Appendix G
4. Click the link: 'CLICK HERE TO BEGIN YOUR APPLICATION'.
5. Click 'Submit' next to 'New Mexico FY 2022 SLCGP Subrecipient Grant Application: Opting Out of State-provided service(s)' and then follow the instructions, including to:
   - **Complete**, **sign**, and **submit** your New Mexico FY 2022 SLCGP direct funding (i.e., 'Opting Out of State-provided service(s)') subrecipient grant application.
   - **Complete** and **submit** the New Mexico FY 2022 SLCGP Subrecipient Project Worksheet. **This document MUST be included with your grant application if you are applying for direct funding for one (1) or more projects.**

III. State-Provided Services AND Direct Funding of Local Government Projects

A. Preparing for the Application Process:

1. **Unique Entity ID:** All applicants **MUST** include a Unique Entity ID (UEI) number when requested on application document(s). If your organization does not have a UEI number or if you need to verify your UEI number visit the SAM.GOV website at: https://sam.gov/content/entity-registration.
2. **Employer Identification Number:** All applicants **MUST** provide an Employer Identification Number (EIN) number when requested on application document(s). Your 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.
3. **New Mexico Statewide Human Resource, Accounting and Management Reporting System (SHARE) Vendor Number**: All applicants **MUST** provide a SHARE vendor number when requested on application document(s). Contact the NMDHSEM Grants Management Bureau for assistance in obtaining a SHARE number: dhsem-grantsmanagement@state.nm.us.

B. Completing the Application Process

1. Visit the NMDHSEM Grants website: https://www.nmdhsem.org/administrative-services-bureau/administrative-services-bureau-grants/.
2. Click on the link for the State and Local Cybersecurity Grant Program.

3. Review:
   - FY 2022 SLCGP Funding Announcement and Allocation Methodology (this document)
   - New Mexico FY 2022 SLCGP Local Consent Agreement form
   - New Mexico FY 2022 SLCGP Project Worksheet form
   - Department of Homeland Security Notice of Funding Opportunity Fiscal Year 2022 State and Local Cybersecurity Grant Program included Appendix G
4. Click the link: 'CLICK HERE TO BEGIN YOUR APPLICATION'.
5. Click 'Submit' next to 'New Mexico FY 2022 SLCGP Subrecipient Grant Application: State-provided service(s)' and then follow the instructions, including to:
   - **Complete**, **sign**, and **submit** your New Mexico FY 2022 SLCGP State-provided service(s) subrecipient grant application.
   - **Complete**, **sign**, and **upload** the New Mexico FY 2022 SLCGP Local Consent Agreement. **This document MUST be included with your grant application if you are applying for one (1) or more projects as State-provided services.**
6. Click 'Submit' next to 'New Mexico FY 2022 SLCGP Subrecipient Grant Application: Opting Out of State-provided service(s)' and then follow the instructions, including to:
   - **Complete**, **sign**, and **submit** your New Mexico FY 2022 SLCGP direct funding (i.e., 'Opting Out of State-provided service(s)') subrecipient grant application.
   - **Complete** and **submit** the New Mexico FY 2022 SLCGP Subrecipient Project Worksheet. **This document MUST be included with your grant application if you are applying for direct funding for one (1) or more projects.**

IV. Application Evaluation Criteria

NMDHSEM will review all grant applications submitted by Eligible Subrecipients for completeness.

The New Mexico Cybersecurity Planning Committee will review grant applications submitted by Eligible Subrecipients seeking direct funding to independently implement projects to ensure they align with the approved projects outlined in the New Mexico Cybersecurity Plan. In doing so, the Cybersecurity Planning Committee will evaluate the applications and project worksheets for (1) adherence to SLCGP programmatic guidelines; (2) anticipated effectiveness of proposed projects; and (3) comprehensiveness and overall quality of the investment justification and project worksheet submitted.

The New Mexico Cybersecurity Planning Committee will make the final decision for awarding SLCGP funds. Final award decisions for fully complete, compliant, and justified applications will be made on a first come first served basis.

G. CONTACT INFORMATION

- NMDHSEM Grants Management Bureau: dhsem-grantsmanagement@state.nm.us
- New Mexico Office of Cybersecurity: cybersecurity.planningcommittee@doit.nm.gov

APPENDIX A: DIRECT FUNDING REQUIREMENTS AND INFORMATION

Eligible Subrecipients applying for direct funding to independently implement projects must comply with the funding restrictions outlined in the FY 2022 SLCGP NOFO. If U.S. DHS or NMDHSEM staff identify costs that are inconsistent with any of these requirements, these costs may be disallowed, and the U.S. DHS may recover funds as appropriate, consistent with applicable laws, regulations, and policies.

1. Cost Share

The U.S. DHS has waived the 10% cost share requirement for New Mexico for the FY 2022 SLCGP. Cost share requirements are not guaranteed to be waived in subsequent years, therefore Eligible Subrecipients opting for direct funding to implement projects independently will have to budget for future cost share requirements (20% for FY 2023 SLCGP, 30% for FY 2024 SLCGP, and 40% for FY 2025 SLCGP).

2. CISA Cyber Hygiene Services

As a condition of receiving SLCGP funding, the Eligible Subrecipient is required to adhere to or sign up for the following services, sponsored by CISA and further described in Appendix G of the FY 2022 SLCGP NOFO. Participation in these services and memberships is not required for submission and approval of a grant application:

- Sign up for cyber hygiene services, specifically vulnerability scanning and web application scanning. To learn more, visit: https://www.cisa.gov/cyber-hygiene-services.

3. Nationwide Cybersecurity Review (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a state, local, or territorial (SLT) entity's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by U.S. DHS and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Subrecipients receiving direct funding and implementing projects independently must complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter. The NCSR is optional but highly encouraged for subrecipients implementing projects as State-provided services. For more information, visit: https://www.cisecurity.org/ms-isac/services/ncsr.

4. SLCGP Funding Restrictions

For FY 2022, SLCGP funds may not be used for any of the following:

a. Spyware;
b. Construction;
c. Renovation;
d. To supplant local funds;
e. For any subrecipient cost-sharing contributions;
f. To pay a ransom;
g. For recreational or social purposes;
h. To pay for cybersecurity insurance premiums;
i. To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities; or
j. For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the subrecipient that receives a grant subaward.

a. Prohibitions for Covered Telecommunications Equipment or Services

Additionally, Eligible Subrecipients **may not** use direct funding to:

a. 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;

b. 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

c. 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 of any system.

See the FY 2022 SLCGP NOFO for the definition of covered telecommunications equipment and services and further explanation on the prohibitions for covered telecommunication equipment or services.

b. Replacement Equipment and Services

Direct funding may be used to procure replacement equipment and services impacted by this prohibition, provided the costs are otherwise consistent with the requirements of the FY 2022 SLCGP NOFO.

5. Allowable Costs

Specific investments made in support of the funding priorities discussed in the FY 2022 SLCGP NOFO generally fall into one of the seven (7) allowable expense categories:

- Planning
- Organization
- Equipment
- Training
- Exercises
- Management and Administration (M&A) costs
- Indirect Facilities and Administrative (F&A) costs

a. Planning

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.

b. Organization

Eligible Subrecipients must justify proposed expenditures of SLCGP funds to support organization activities within their investment justifications. 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 to perform allowable SLCGP POETE (planning, organization, equipment, training, and exercise) activities. Personnel expenses may include, but are not limited to training and exercise coordinators, program managers and planners, and cybersecurity navigators. The Eligible Subrecipient must demonstrate that the personnel will be sustainable once the program ends or funds are no longer available.

c. **Equipment**

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 U.S. DHS standards. In addition, Eligible Subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

See the FY 2022 SLCGP NOFO for additional and specific information on this topic.

d. **Training**

Allowable training-related costs 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 New Mexico Cybersecurity Plan and address a performance gap identified through assessments and that contributes to building a capability that will be evaluated through a formal exercise.

See the FY 2022 SLCGP NOFO for additional and specific information on this topic.

e. **Exercises**

Exercises conducted with SLCGP funding should be managed and conducted consistent with the Homeland Security Exercise and Evaluation Program (HSEEP).

See the FY 2022 SLCGP NOFO for additional and specific information on this topic.

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

M&A activities are allowable under this program. These 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 subrecipient of the funding passed through by the State solely for M&A purposes associated with the SLCGP sub-award.

g. **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. See the FY 2022 SLCGP NOFO for additional information on Indirect Facilities & Administrative Costs.

6. **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).

If a subrecipient uses SLCGP funding to support emergency communications investments, the following requirements shall apply to all such grant-funded communications investments in support of emergency communications priorities and recognized best practices:

- The signatory authority for the Eligible Subrecipient must certify in writing to U.S. DHS/FEMA their compliance with the SAFECOM Guidance. The certification letter should be coordinated with the Statewide Interoperability Coordinator (SWIC) for New Mexico and must be uploaded to the ND Grants system at the time of New Mexico's first Program Performance Report (PPR) submission, as informed by the Eligible Subrecipient's associated Quarterly Performance Report.

7. **DHS Standard Terms and Conditions**
   All successful applicants for U.S. DHS grants and cooperative agreements are required to comply with DHS Standard Terms and Conditions, which are available online at: DHS Standard Terms and Conditions.