

# State of New Mexico

State and Local Cybersecurity Grant Program  
(SLCGP) – Subrecipient Application

# State and Local Cybersecurity Grant Program (SLCGP)

## Background

- The U.S. Department of Homeland Security (DHS) is **providing funding** to address **cybersecurity risks and threats** to information systems of State, Local, and Territorial (SLT) governments.
- The New Mexico Cybersecurity Planning Committee ('Planning Committee') conducted a **statewide Capabilities Assessment** to identify **cybersecurity gaps** within **133 Local & Tribal governments**.
- The Planning Committee documented and approved the **New Mexico Cybersecurity Plan** to strategize an approach to **address capability gaps** found by the Assessment and **enhance cybersecurity posture** across New Mexico.
- The Planning Committee identified and prioritized—and is coordinating with the New Mexico Office of Cybersecurity to provide—**five (5) cybersecurity projects** for eligible subrecipients as **statewide services** to address **key capability gaps** and **maximize return on investment**.

# SLCGP Project Options

## Available Projects for Year 1

Eligible subrecipients (e.g., counties, cities, towns, K-12 school districts, tribal entities) can apply for one (1) or more of the following five (5) cybersecurity projects approved by the New Mexico Cybersecurity Planning Committee:

### AVAILABLE PROJECTS

---

- 1 Cybersecurity Governance and Planning**
  - Assistance with establishing or enhancing cybersecurity governance and implementing or expanding cyber best practices / cyber hygiene
- 2 Cybersecurity Risk Assessments**
  - Assistance with performing cybersecurity risk assessments to understand cybersecurity posture and identify cyber risks and gaps
- 3 Vulnerability and Attack Surface Management**
  - Receive services for mitigating cybersecurity risks through deployment and integration of vulnerability and attack surface management capabilities
- 4 Cybersecurity Training**
  - Obtain basic cybersecurity awareness and phishing training for employees
- 5 Cybersecurity Workforce Development Planning**
  - Participate in development of a strategic plan and roadmap for assessing and improving cybersecurity workforce capabilities using the Workforce Framework for Cybersecurity (NICE Framework)

# SLCGP Subrecipient Requirements

## Subrecipient Requirements by Grant Application Option

Eligible subrecipients implementing the approved SLCGP project(s) will be subject to grant requirements associated with their chosen application option. *The Planning Committee encourages eligible entities to apply for cybersecurity projects as **State-provided services**.*

### SUBRECIPIENT REQUIREMENTS

#### 1 State-provided Services

- Implement **cybersecurity services and capabilities provided** by the New Mexico Office of Cybersecurity
- Coordinate with the NM Office of Cybersecurity to **scope and define** project requirements
- Complete, sign, and submit the **Local Consent Agreement** to the New Mexico Department of Homeland Security and Emergency Services (must be completed by an “authorized official”)

#### 2 Opting Out of State-provided Service(s)

- Responsible for any SLCGP **cost share** requirements
- Complete **Investment Justification (IJ)** and **Project Worksheet (PW)** to implement SLCGP project(s) that meet the goals of the NM Cybersecurity Plan\*
- Fulfill **quarterly programmatic** and **financial reporting and documentation** requirements
- Subject to **audit and oversight reviews**, as required by the grant program

#### 3 Hybrid Option

- Fulfill requirements outlined for **both** Options 1 and 2

\*The NM statewide Cybersecurity Plan is available at: [New Mexico Cybersecurity Plan](https://api.realfile.rtsclients.com/PublicFiles/16569e3bf98c467e95901b46fd511499/6c75dd2a-2007-4645-8b91-d4c80423048b/Approved_Cybersecurity_Plan.pdf) ([https://api.realfile.rtsclients.com/PublicFiles/16569e3bf98c467e95901b46fd511499/6c75dd2a-2007-4645-8b91-d4c80423048b/Approved\\_Cybersecurity\\_Plan.pdf](https://api.realfile.rtsclients.com/PublicFiles/16569e3bf98c467e95901b46fd511499/6c75dd2a-2007-4645-8b91-d4c80423048b/Approved_Cybersecurity_Plan.pdf))

# Subrecipient Participation

## Subrecipient Applications and Additional Information

Subrecipients wishing to participate in the SLCGP may use the following QR codes or URLs:



[NMDHSEM  
SLCGP website](https://www.nmdhsem.org/state-and-local-cybersecurity-grant-program-slcgp/)

[\(https://www.nmdhsem.org/state-and-local-cybersecurity-grant-program-slcgp/\)](https://www.nmdhsem.org/state-and-local-cybersecurity-grant-program-slcgp/)



[State-provided  
Service\(s\) application](https://nmdhsem.submittable.com/ogin?returnUrl=%2Fsubmit%2F285225%2Fnew-mexico-fy-2022-state-and-local-cybersecurity-grant-program-slcgp-grant-appl)

[\(https://nmdhsem.submittable.com/ogin?returnUrl=%2Fsubmit%2F285225%2Fnew-mexico-fy-2022-state-and-local-cybersecurity-grant-program-slcgp-grant-appl\)](https://nmdhsem.submittable.com/ogin?returnUrl=%2Fsubmit%2F285225%2Fnew-mexico-fy-2022-state-and-local-cybersecurity-grant-program-slcgp-grant-appl)



[Opting Out of State-provided  
Service\(s\) application](https://nmdhsem.submittable.com/ogin?returnUrl=%2Fsubmit%2F285226%2Fnew-mexico-fy-2022-state-and-local-cybersecurity-grant-program-slcgp-grant-appl)

[\(https://nmdhsem.submittable.com/ogin?returnUrl=%2Fsubmit%2F285226%2Fnew-mexico-fy-2022-state-and-local-cybersecurity-grant-program-slcgp-grant-appl\)](https://nmdhsem.submittable.com/ogin?returnUrl=%2Fsubmit%2F285226%2Fnew-mexico-fy-2022-state-and-local-cybersecurity-grant-program-slcgp-grant-appl)

For additional information, you can also email the New Mexico Cybersecurity Planning Committee at: [cybersecurity.planningcommittee@doit.nm.gov](mailto:cybersecurity.planningcommittee@doit.nm.gov)

**NMDHSEM's SLCGP website**



# STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP)

[Home](#) » State and Local CyberSecurity Grant Program (SLCGP)

## STATE AND LOCAL CYBERSECURITY GRANT PROGRAM (SLCGP) 2022

### Purpose

The federal [Infrastructure Investment and Jobs Act \(IIJA\)](#), also known as the Bipartisan Infrastructure Law (BIL), was signed into law on November 15, 2021. One component of the act is the State and Local Cybersecurity Grant Program (SLCGP), which appropriated \$1 billion over four years (2022-2025) to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

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. 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.





## VIEW AND DOWNLOAD DOCUMENTS

2022 SLCGP Local Funding Announcement and Allocation Methodology

Required to be completed, signed, and submitted by subrecipients that choose to apply for one or more State-provided projects ("State-provided service(s)")

New Mexico Local Consent Form

Required to be completed and submitted by subrecipients that choose to request subaward for independently performing one or more SLCGP projects (i.e., "Opting Out of State-provided service(s)")

Sub-Recipient Project Worksheet

2022 Federal SLCGP Notice of Funding Opportunity (NOFO)

Provides comprehensive information on the SLCGP for potential grant subrecipients in New Mexico, including on:

- Purpose, objectives, and priorities of SLCGP in NM
- Eligibility criteria for SLCGP subrecipients
- Approved FY 2022 SLCGP projects and application options
- Grant application instructions
- Additional requirements for applications for direct funding assistance ("Opting Out of State-provided service(s)")

Environmental and Historic Preservation Screening Form

Authorized Equipment List:

[www.fema.gov/grants/guidance-tools/authorized-equipment-list](http://www.fema.gov/grants/guidance-tools/authorized-equipment-list)

Federal notice of grant funding opportunity for the entire FY 2022 SLCGP and all 'eligible entities' (i.e., states and territories) and eligible grant subrecipients (i.e., local governments)

**CLICK HERE TO BEGIN YOUR APPLICATION**





# New Mexico Department of Homeland Security and Emergency Management

The New Mexico Department of Homeland Security and Emergency Management (DHSEM), also recognized as the State Administering Agency (SAA), administers two categories of federal grant funding:

- 1) Disaster grants enable state, tribal, and local governments, as well as certain non-profit organizations, to respond and recover from major disasters and emergencies as quickly as possible. Typically, these grants are only available after the President of the United States declares a major disaster and authorizes the grants.
- 2) Non-Disaster grants are primarily designed to enhance the capacity of state and local emergency responders to prevent and mitigate the effects of various hazards, such as wildfires, drought, flash flooding, and domestic violent extremism. These grants can address a wide variety of preparedness efforts, including public awareness campaigns, repairs of critical infrastructure, and improvements to emergency response systems, among others.

DHSEM coordinates around the mission areas of the National Preparedness Goal: prevention, protection, mitigation, response, and recovery from all hazard types.

This application is supported with funding provided by the U.S. Department of Homeland Security.

## New Mexico FY 2022 State and Local Cybersecurity Grant Program (SLCGP) Grant Application: State-provided service(s)

Ends on Wed, May 1, 2024 2:00 AM

Submit

## New Mexico FY 2022 State and Local Cybersecurity Grant Program (SLCGP) Grant Application: Opting Out of State-provided service(s)

Ends on Wed, May 1, 2024 2:00 AM

Submit

Link to begin grant application process for one or more SLCGP projects as "State-provided service(s)"

Link to begin grant application process to request subaward for independently performing one or more SLCGP projects (i.e., "Opting Out of State-provided service(s)")

Utilize both grant application links if applying for one or more SLCGP projects as a "State-provided service(s)" AND requesting a subaward to independently perform one or more SLCGP projects (i.e., "Opting Out of State-provided service(s)")

*\*An applicant should NOT apply for the same project(s) as both a "State-provided service" and as a subaward to perform that same project(s) on its own*

**“State-provided service(s)”  
grant application steps**



# New Mexico Department of Homeland Security and Emergency Management

1



New Mexico FY 2022 State and Local Cybersecurity Grant Program (SLCGP) Grant Application: State-provided service(s)  
Ends on Wed, May 1, 2024 2:00 AM

## About Your Organization

If you have any questions, please reach out to [cybersecurity.planningcommittee@doit.nm.gov](mailto:cybersecurity.planningcommittee@doit.nm.gov)

First section of grant application form requires various information about applicant organization

Red, bold asterisk (\*) indicates a required field

An important field for the SLCGP as a *minimum* of 25% of total grant funding *must* benefit rural jurisdictions (less than 50,000 in total population)

Organization Name: \*

Organization Type: \*

Address: \*

Building or Suite Number:

City: \*

Zip Code: \*

County: \*

### Is your Organization a Rural area? \*

- Rural area (Less than 50,000 population)
- Not a Rural area (Over 50,000 population)

## Executive Sponsor / Authorizing Official \*

2

First Name

Last Name

*This individual will need to sign the Local Consent Agreement.*

Title: \*

Email Address: \*

Work Phone: \*

Primary Organization Point of Contact for SLCGP Grant Request:

First Name

Last Name

*Name & contact information for this role is not required if same as the Executive Sponsor / Authorizing Official*

Title:

Email Address:

Work Phone:

Primary Technical (IT) Point of Contact:

First Name

Last Name

*Name & contact info. for this role is not required if same as the Executive Sponsor / Authorizing Official and/or Primary Org. POC for SLCGP*

Email Address:

Work Phone:

## About Your Organization

If you have any questions, please reach out to [cybersecurity.planningcommittee@doit.nm.gov](mailto:cybersecurity.planningcommittee@doit.nm.gov)

Main organization website address:

example.com

Organization domains/subdomains:

example.com

Organization public IP addresses/ranges:

Total number of supported users:

(employees and contractors only; do not include students)

Total number of staff members dedicated to IT and/or cybersecurity:

(employees and contractors)

How much is your total Annual IT Budget?

Please use the following format: \$1,000.00

How much is your total Annual Cybersecurity Budget?

Please use the following format: \$1,000.00

Total number of physical sites/locations:

3

Additional, non-mandatory fields for capturing organizational information

## About Your Information Technology Department

If you have any questions, please reach out to [cybersecurity.planningcommittee@doit.nm.gov](mailto:cybersecurity.planningcommittee@doit.nm.gov)

Total number of laptops and desktop computers:

Total number of servers:

Are your IT/OT environments managed by in-house staff or outsourced to a third party?

- Managed by Staff  
 Managed by 3rd Party

Do you use a public cloud service provider(s) to host critical information technology systems and/or sensitive information?

- Yes  
 No

In addition to information technology assets, does your organization also implement and manage operational technologies (OT)?

- Yes  
 No

Operational technologies consist of computing systems used to help manage, monitor, and control physical operations such as building management systems, public transportation systems, public safety systems, water and wastewater treatment systems, public lighting systems, electrical generation and transmission, etc.

For your IT and OT environments, please list the operating systems and versions in use:

What is your biggest motivation(s) / reason(s) to apply for this grant opportunity?

4

Non-mandatory fields for capturing information about the organization's IT & OT environments

Section of application for selecting State-provided service(s) for which an organization would like to participate

## CYBERSECURITY PROJECTS

5

Please indicate which State-provided, FY 2022 SLCGP project(s) you are applying for: \*

- Cybersecurity Governance Planning
- Cybersecurity Risk Assessments
- Vulnerability and Attack Surface Management
- Cybersecurity Training
- Cyber Workforce Development Planning

Select one or more State-provided, FY 2022 SLCGP cybersecurity project(s) by clicking on the associated checkbox(es)

- **Cybersecurity Governance 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).
- **Cybersecurity Risk Assessments:** Obtain assistance in performing cybersecurity risk assessments utilizing the Nationwide Cybersecurity Review (NCSR), etc. to understand the entity's 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.
- **Vulnerability and Attack Surface Management:** Obtain services resulting from the deployment and integration of vulnerability and attack surface management capabilities for mitigating cybersecurity risks.
- **Cybersecurity Training:** Obtain basic cybersecurity awareness and phishing training for employees.
- **Cyber 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.

Please upload the signed Local Consent Agreement. \*

Choose File

Upload a file. No files have been attached yet.

Acceptable file types: .csv, .doc, .docx, .odt, .pdf, .rtf, .txt, .wpd, .wpl, .gif, .jpg, .jpeg, .png, .svg, .tif, .tiff

You can find the Consent Form form available [HERE](#).

Upload field (including "drag and drop" functionality) for uploading completed and signed Local Consent Agreement form

Link to access and download fillable Local Consent Agreement .pdf form

*[Information on the Local Consent Agreement form is also provided in the next slide]*

I understand that the submission of this application does not guarantee that my organization will receive the services or resources requested. I understand that each application received will be evaluated in accordance with DHS/FEMA SLCGP requirements and those of the New Mexico Cybersecurity Planning Committee. \*

Please type your full name \*

First Name

Last Name

Today's Date \*

Save Draft Submit

Checkbox indicating acknowledgement that there is no guarantee the organization will receive the services or resources requested

Buttons for saving your draft application OR submitting your final application, once complete

**State of New Mexico  
Federal Fiscal Year 2022  
State and Local Cybersecurity Grant Program  
Local Consent Agreement**

I, \_\_\_\_\_ (printed name), the authorized official on behalf of \_\_\_\_\_ (the "Local Governmental Entity"), located at \_\_\_\_\_ (address) hereby **expressly consent** to the State of New Mexico's State Administrative Agency (SAA), namely the New Mexico Department of Homeland Security and Emergency Management (NM DHSEM), on behalf of the New Mexico Office of Cybersecurity (NM OCS), undertaking the following acts in accordance with the State and Local Cybersecurity Grant Program (SLCGP) for federal Fiscal Year (FY) 2022. Funding Opportunity Number DHS-22-137-000-01, as authorized by Section 2220A of the Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g):

1. Passing through items, services, capabilities, and activities in lieu of federal funding to local governments and rural areas on a statewide basis and with a minimum value of:
  - a. For local governments: \$2,032,322.40 total, or 80% of the State of New Mexico's total FY 2022 SLCGP federal grant award of \$2,540,403.00
  - b. For rural areas: \$635,100.75 total, or 25% of New Mexico's total FY 2022 federal grant award

2. Utilizing FY 2022 SLCGP grant funding for the following projects approved in the State of New Mexico Cybersecurity Plan on behalf and for the benefit of local governments (including rural areas):
  - a. \$450,000.00 total for Cybersecurity Governance and Planning
  - b. \$500,000.00 total for Cybersecurity Risk Assessments
  - c. \$488,000.00 total for Vulnerability and Attack Surface Management
  - d. \$250,000.00 total for Cybersecurity Training
  - e. \$150,383.00 total for Cybersecurity Workforce Development Planning

*(Please click on the check box(es) associated with the project(s) for which your Local Governmental Entity would like to participate in/benefit from.)*

Select one or more State-provided, FY 2022 SLCGP cybersecurity project(s) by clicking on the associated checkbox(es)

This consent is given freely and with the understanding that the Local Governmental Entity is receiving items, services, capabilities, and activities (e.g., hardware, software, services) in lieu of direct funding from the State of New Mexico's FY 2022 SLCGP grant award. This consent is *only* effective for FY 2022 SLCGP federal funds and applies *only* to that portion of federal funding that will specifically benefit the Local Governmental Entity.

It's important that the "Authorized Official" for the applicant organization sign and date the completed Local Consent Agreement form  
*\*A digital signature may be used to sign this form*

Signed,

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date:

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

Available at:

[https://www.nmdhsem.org/wp-content/uploads/2024/02/New-Mexico-Local-Consent-Form\\_15Nov2023.pdf](https://www.nmdhsem.org/wp-content/uploads/2024/02/New-Mexico-Local-Consent-Form_15Nov2023.pdf)

# **“Opting Out of State-provided service(s)” grant application steps**



# New Mexico Department of Homeland Security and Emergency Management

1



New Mexico FY 2022 State and Local  
Cybersecurity Grant Program (SLCGP) Grant  
Application: Opting Out of State-provided  
service(s)

Ends on Wed, May 1, 2024 2:00 AM

## First, let's find your organization

All applicants must apply on behalf of a registered organization. [Learn more about organization registration requirements](#)

Organization EIN or UEI \*

e.g. 12-3456789 for EIN or ABCDE1234567 for UEI.

Search organizations



The process starts with an applicant organization finding and leveraging its Employer Identification Number (EIN) or Unique Entity Identifier (UEI)

*\*Applicant organizations must have both an EIN and a UEI to receive an SLCGP grant subaward*







# New Mexico Department of Homeland Security and Emergency Management

2

New Mexico FY 2022 State and Local Cybersecurity Grant Program (SLCGP) Grant Application: Opting Out of State-provided service(s)  
Ends on Wed, May 1, 2024 2:00 AM



Applying on behalf of:

**[Government Entity Name]**  
 EIN: [Redacted]  
 Address: [Redacted]  
[Change organization](#) [Learn how to manage organization details](#)

Powered by Candid © 2024 Candid

Organization Name: \*

[Redacted] Limit: 300 characters

Red, bold asterisk (\*) indicates a required field

Organization Type: \*

Select...

Verify that organization name matches the EIN or UEI supplied in the previous screen  
*\*Can change organization, as necessary*

Organization Address: \*

[Redacted]

Organization Building / Suite:

[Redacted]

An important field for the SLCGP as a *minimum of 25%* of total grant funding *must* benefit rural jurisdictions (less than 50,000 in total population)

Organization City: \*

[Redacted]

A link is provided to an IRS website for obtaining an EIN if an organization does not already have an EIN

3

Organization Zip Code: \*

[Redacted]

Employer Identification Number: \*

[Redacted]

An 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>

Unique Entity Identifier: \*

[Redacted]

UEI registration information is available on GSA.gov at:  
<https://sam.gov/content/entity-registration>

A link is provided to a GSA website (SAM.gov) for registering for a UEI if an organization does not already have a UEI

New Mexico SHARE Vendor Number: \*

[Redacted]

As necessary, please contact the NMDHSEM Grants Management Bureau for assistance in obtaining a New Mexico SHARE (Statewide Human Resource, Accounting and Management Reporting System) vendor number at: [dhsem-grantsmanagement@state.nm.us](mailto:dhsem-grantsmanagement@state.nm.us)

County: \*

Select...

Do you have a negotiated indirect cost rate?

Yes  
 No

If an organization has a negotiated indirect cost rate, it may be able to use a percentage of its subaward for indirect (e.g., admin) costs

Is your Organization a Rural area? \*

Rural area (Less than 50,000 population)  
 Not a Rural area (Over 50,000 population)

A DHSEM email address is provided for obtaining a SHARE vendor number if an organization does not already have a SHARE vendor number

**Executive Sponsor / Authorizing Official** \*

4

First Name

Last Name

Title: \*

Email Address: \*

Work Phone: \*

**Primary Organization Point of Contact for SLCGP Grant Request:**

First Name

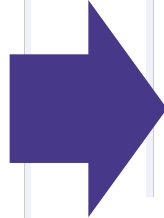
Last Name

*Name & contact information for this role is not required if same as the Executive Sponsor / Authorizing Official*

Title:

Email Address:

Work Phone:



**Primary Technical (IT) Point of Contact:**

5

First Name

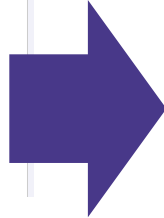
Last Name

*Name & contact info. for this role is not required if same as the Executive Sponsor / Authorizing Official and/or Primary Org. POC for SLCGP*

Title:

Email Address:

Work Phone:



## About Your Organization

If you have any questions, please reach out to [cybersecurity.planningcommittee@doit.nm.gov](mailto:cybersecurity.planningcommittee@doit.nm.gov)

Main organization website address:

example.com

Organization domains/subdomains:

example.com

Organization public IP addresses/ranges:

Total number of supported users:

(employees and contractors only; do not include students)

Total number of staff members dedicated to IT and/or cybersecurity:

(employees and contractors)

How much is your total Annual IT Budget?

Please use the following format with dollars and cents: \$1,000.00

How much is your total Annual Cybersecurity Budget?

Please use the following format with dollars and cents: \$1,000.00

Total number of physical sites/locations:

6

Additional, non-mandatory fields for capturing organizational information

## About Your Information Technology Department

Total number of laptops and desktop computers:

Total number of servers:

Are your IT/OT environments managed by in-house staff or outsourced to a third party?

- Managed by Staff  
 Managed by 3rd Party

Do you use a public cloud service provider(s) to host critical information technology systems and/or sensitive information?

- Yes  
 No

In addition to information technology assets, does your organization also implement and manage operational technologies (OT)?

- Yes  
 No

Operational technologies consist of computing systems used to help manage, monitor, and control physical operations such as building management systems, public transportation systems, public safety systems, water and wastewater treatment systems, public lighting systems, electrical generation and transmission, etc.

For your IT and OT environments, please list the operating systems and versions in use:

What is your biggest motivation(s) / reason(s) to apply for this grant opportunity?

7

Non-mandatory fields for capturing information about the organization's IT & OT environments

## CYBERSECURITY PROJECTS

Provide a baseline understanding of the existing cybersecurity gaps, risks, and threats that the applicant entity faces which have influenced the development of this sub-recipient Investment Justification (IJ). \*

Section of application for selecting State-provided service(s) for which an organization would like to participate

Please include a summary of the current capabilities within the applicant jurisdiction to address these threats and risks. \*

Describe how this IJ and the associated project(s) addresses existing cybersecurity gaps, risks, and threats. \*

Please indicate which FY 2022 SLCGP project(s) you are applying for: \*

- Cybersecurity Governance Planning
- Cybersecurity Risk Assessments
- Vulnerability and Attack Surface Management
- Cybersecurity Training
- Cyber Workforce Development Planning

- **Cybersecurity Governance 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).
- **Cybersecurity Risk Assessments:** Obtain assistance in performing cybersecurity risk assessments utilizing the Nationwide Cybersecurity Review (NCSR), etc. to understand the entity's 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.
- **Vulnerability and Attack Surface Management:** Obtain services resulting from the deployment and integration of vulnerability and attack surface management capabilities for mitigating cybersecurity risks.
- **Cybersecurity Training:** Obtain basic cybersecurity awareness and phishing training for employees.
- **Cyber 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.

Select one or more State-provided, FY 2022 SLCGP cybersecurity project(s) by clicking on the associated checkbox(es)

8

## Cybersecurity Governance Planning

16 Required Cybersecurity Elements as detailed in FY 2022 SLCGP NOFO: Please describe how this project aligns to the cybersecurity elements in Appendix C of the FY 2022 SLCGP NOFO and the New Mexico Cybersecurity Plan. \*

FY 2022 SLCGP NOFO is available at: <https://www.fema.gov/fact-sheet/department-homeland-security-notice-funding-opportunity-fiscal-year-2022-state-and-local>

New Mexico Cybersecurity Plan is located here.

A link is provided to the New Mexico Cybersecurity Plan

Funding amount requested for project: \*

Please use the following format with dollars and cents: \$1,000.00

The implementation schedule table should be used as a planning tool for the key activities associated with each project in the New Mexico Cybersecurity Plan. For each project and each year of the grant, the applicant should include the activities necessary to meet the goals of each project, as well as the estimated start and completion dates (by calendar quarter) for each activity.

The standard definition of a project is a temporary endeavor with a defined beginning and end (usually time-constrained, constrained by funding or a deliverable), undertaken to meet unique goals and objectives, typically to bring about beneficial change or added value. Applying this standard to projects using preparedness grant funds, a project is a related set of activities and purchases supporting the building or sustaining of core capabilities, and is associated with a single entity responsible for execution.

This approach will allow NMDHSEM and the applicant to categorize a grant-funded project as a discrete unit for post-award management, reporting, and monitoring purposes. The main steps and processes of the Project Management Lifecycle (PML) are Initiate, Execute, Control, and Close Out.

- **Initiate:** The authorization to begin work or resume work on any particular activity.
- **Execute:** The period within the project life cycle during which the actual work of creating the project's deliverables is carried out.
- **Control:** A mechanism which reacts to the current project status to ensure accomplishment of project objectives. This involves planning, measuring, monitoring, and taking corrective action based on the results of the monitoring.
- **Close Out:** The completion of all work on a project; can also refer to completion of a phase of the project.

For additional information on the Project Management Lifecycle, please visit Project Management Institute's (PMI) *A Guide to the Project Management Body of Knowledge (PMBOK Guide)* at <http://www.pmi.org/PMBOK-Guide-and-Standards.aspx>. Specifically, applicants are encouraged to reference Chapter three of the PMBOK Guide, *The Standard for Project Management of a Project*.

Which Project Management step applies to you? \*

- Initiate
- Execute
- Control
- Close Out

When is the start date for completion of the project milestones? \*

☐

When is the end date for completion of the project milestones? \*

☐

Required project management-related information

\*See link provided above to PMBOK Guide to learn more about the Project Management Lifecycle and associated concepts

9

URL for the FY 2022 SLCGP NOFO issued by FEMA is provided

\*See Appendix C of NOFO

Please upload your completed Project Worksheet form. \*

Choose File

Upload a file. No files have been attached yet.

Acceptable file types: .csv, .doc, .docx, .odt, .pdf, .rtf, .txt, .wpd, .wpl, .gif, .jpg, .jpeg, .png, .svg, .tif, .tiff

You can find the Project Worksheet form available [HERE](#).

I understand that any SLCGP sub-recipient that opts out of a project as a State-provided service and chooses to implement the project on its own will be responsible for any associated project cost share requirements prescribed by the Federal Emergency Management Agency (FEMA); Quarterly  Performance Reports (QPR) due to the New Mexico the Department of Homeland Security and Emergency Management (NMDHSEM) by January 15, April 15, July 15, and October 15th each year; and Quarterly Financial Reports (QFR) due to NMDHSEM by January 15th, April 15th, July 15th, and October 15th each year.

I understand that the submission of this application does not guarantee that my organization will receive the resources requested. I understand that each application received will be evaluated in  accordance with U.S. Department of Homeland Security (DHS) / Federal Emergency Management Agency (FEMA) SLCGP requirements and those of the New Mexico Cybersecurity Planning Committee.

Please type your full name \*

First Name

Last Name

Today's Date \*

Save Draft

Submit

Last Saved 4 minutes ago

10

Upload field (including "drag and drop" functionality) for uploading completed Project Worksheet form

Link to access and download fillable Project Worksheet .xlsx form

*[Information on the Project Worksheet (PW) form is also provided in the next two slides]*

Checkbox indicating acknowledgement that there is no guarantee the organization will receive the resources requested

Checkbox indicating acknowledgement that an organization that opts out of State-provided service(s) and chooses to implement one or more FY 2022 SLCGP projects on its own is **responsible for any cost share requirements**, as well as for required **quarterly project performance and financial reporting** to NMDHSEM

Buttons for saving your draft application **OR** submitting your final application, once complete

# Project Worksheet – Tab 1 (Organization & POC Info. and Guidance)

AutoSave Off | New Mexico FY 2022 SLCGP Sub-Recipient Project Worksheet template.xlsx • Saved to this PC

File Home Insert Draw Page Layout Formulas Data Review View Automate Help ANALYTICS AUDIT TOOL Acrobat | Comments | Share

C3

Confidential \ No Additional Protection

	A	B	C	D	E	F	G	H	I	
1	<b>New Mexico FY 2022 SLCGP Sub-Recipient Project Worksheet Guidance</b>									
2	Complete rows 3-8 with the organization's information.									
3	<b>Organization Name</b>									
4	<b>POC Name:</b>									
5	<b>POC Title:</b>									
6	<b>Organization Address:</b>									
7	<b>POC Phone Number:</b>									
8	<b>POC Email Address:</b>									
9	The table below provides a brief overview of the two tabs in the SLCGP Project Worksheet.									
10	<b>Worksheet</b>	<b>Column</b>			<b>Guidance</b>			<b>Purpose</b>		
11	<b>Baseline Project Information</b>	This tab requires the applicant to provide: <b>A)</b> Eligible Applicant Name; <b>B)</b> FY 2022 SLCGP Project(s) Name; <b>C)</b> FY 2022 SLCGP Project(s) Alignment to 16 Required Cybersecurity Elements; <b>D)</b> FY 2022 SLCGP Project Description; <b>E)</b> Project Location (Zip Code); <b>F)</b> Federal Amount; <b>G)</b> Cost Share; <b>H)</b> Total Project Costs			<b>Column B:</b> Project names have been pre-populated to reflect the five (5) projects approved by the New Mexico Cybersecurity Planning Committee as part of the FY 2022 SLCGP and included in the State of New Mexico Cybersecurity Plan approved by the Cybersecurity and Infrastructure Security Agency (CISA).  <b>Column G:</b> For the FY 2022 SLCGP, a Cost Share Waiver was approved by the Federal Emergency Management Agency (FEMA) so NO Cost Share is required. (Column G is pre-populated at \$0 for each potential project accordingly.)  <b>Column H:</b> Data is populated throughout the tabs for reference of how to complete form. Ensure all formulas and totals are aligned under <b>Total Project Costs</b> .			Project Information		
12	<b>Project Implementation</b>	This worksheet requires outlining key project activities and tasks associated with each project identified in the IJ. For application, the estimated start and completion dates ( <b>by calendar quarter</b> ) should be included on the schedule. This sheet should also be used for quarterly reporting on grant activities. For progress reporting purposes, the actual start and completion dates ( <b>by calendar quarter</b> ) should be included on the schedule.							Project Implementation	
13	<b>CONFIDENTIALITY</b>									
14	As some of the information you provide in your SLCGP Investment Justification (IJ) will inherently include administrative or technical information which, if disclosed would jeopardize computer security, portions of this application are deemed confidential and exempt from Inspection of Public Record (IPRA).									

Guidance | Baseline Project Information | Project Implementation

Available at:

[https://www.nmdhsem.org/wp-content/uploads/2024/02/New-Mexico-FY-2022-SLCGP-Sub-Recipient-Project-Worksheet-template\\_15Dec2023.xlsx](https://www.nmdhsem.org/wp-content/uploads/2024/02/New-Mexico-FY-2022-SLCGP-Sub-Recipient-Project-Worksheet-template_15Dec2023.xlsx)

# Project Worksheet – Tabs 2 & 3 (Project-specific information)

## Tab 2:

AutoSave Off | New Mexico FY 2022 SLCGP Sub-Recipient Project Worksheet t... | Saved to this PC | Comeau, Rick

File Home Insert Draw Page Layout Formulas Data Review View Automate Help ANALYTICS AUDIT TOOL Acrobat

A20

Confidential \ No Additional Protection

A	B	C	D	E	F	G	H	I	J
Eligible Applicant Name	FY 2022 SLCGP Project(s) Name	FY 2022 SLCGP Project(s) Alignment to 16 Required Cybersecurity Elements	FY 2022 SLCGP Project Description	Project Location (ZIP Code)	Federal Amount (whole dollars only)	Cost Share (whole dollars only)*	Total Project Costs (Federal + Cost Share) (whole dollars only)		
	Cybersecurity Governance and Planning					\$0	\$0		
	Cybersecurity Risk Assessments					\$0	\$0		
	Vulnerability and Attack Surface Management					\$0	\$0		
	Cybersecurity Training					\$0	\$0		
	Cybersecurity Workforce Development Planning					\$0	\$0		
						\$0	\$0		
						\$0	\$0		

Guidance **Baseline Project Information** Project Implementation

Ready Accessibility: Investigate

## Tab 3:

AutoSave Off | New Mexico FY 2022 SLCGP Sub-Recipient Project Worksheet t... | Saved to this PC | Comeau, Rick

File Home Insert Draw Page Layout Formulas Data Review View Automate Help ANALYTICS AUDIT TOOL Acrobat

A2

Confidential \ No Additional Protection

A	B	C	D	E	F	G	H	I	J	K	L
Eligible Applicant Name	FY 2022 SLCGP Project(s) Name	FY 2022 SLCGP Project Description	Project Management Step	Start Date	End Date	Federal Amount (whole dollars only)	Cost Share (whole dollars only)	Total Project Costs (Federal + Cost Share) (whole dollars only)			
	Cybersecurity Governance and Planning					\$0	\$0	\$0			
	Cybersecurity Risk Assessments					\$0	\$0	\$0			
	Vulnerability and Attack Surface Management					\$0	\$0	\$0			
	Cybersecurity Training					\$0	\$0	\$0			
	Cybersecurity Workforce Development Planning					\$0	\$0	\$0			
						\$0	\$0	\$0			

Guidance Baseline Project Information **Project Implementation**

Ready Accessibility: Investigate

# Required Quarterly Reporting for SLCGP Subrecipients

- An organization that **opts out of a State-provided project(s) and receives an SLCGP subaward to implement one or more projects on its own will be required to submit quarterly performance and financial reports** to the New Mexico Department of Homeland Security & Emergency Management (NMDHSEM)
- **Quarterly Performance Reports (QPR)** may include:
  - Brief narrative of overall project(s) status
  - Summary of project expenditures
  - Description of any potential issues that may affect project completion
  - Metrics data collected for NMDHSEM performance measures
- **Quarterly Financial Reports (QFR)** may include information on:
  - Cash receipts and cash disbursements
  - Total federal funds authorized, federal share of expenditures, federal share of unliquidated obligations, and unobligated balance of federal funds
  - Any subrecipient share required, subrecipient share of expenditures, and remaining recipient share to be provided
  - Any indirect expenses
- QPRs and QFRs will be due to NMDHSEM by **January 15<sup>th</sup>, April 15<sup>th</sup>, July 15<sup>th</sup>, and October 15<sup>th</sup> each year.**



# Obtaining an EIN, UEI and/or NM SHARE vendor number

- **Employer Identification Number (EIN)**
  - An EIN is required for all SLCGP award subrecipients
  - An organization should visit the IRS's website to register for an EIN if it does not already have one
  - An 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>
- **Unique Entity Identifier (UEI)**
  - A UEI is also required for all SLCGP award subrecipients
  - An organization should visit the GSA-managed, SAM.gov website to register for a UEI if it does not already have one
  - UEI registration information is available at the following website: <https://sam.gov/content/entity-registration>
- **New Mexico SHARE vendor number**
  - A NM SHARE vendor number is also required for all SLCGP award subrecipients
  - If it does not already have one, an organization can obtain a NM SHARE vendor number by emailing the NMDHSEM Grants Management Bureau at: [dhsem-grantsmanagement@state.nm.us](mailto:dhsem-grantsmanagement@state.nm.us)