Email This Preview Save as PDF Print Close Window A▲▼

Powered by ZoomGrants™ and

Nevada Office of Emergency Management / Homeland Security

FFY 2025 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/1/2025

City of Reno

XDR Proactive Hardening and Attack Surface Reduction (PHASR)

Jump to: Pre-Application Application Questions Category Budget Totals Line Item Detail Budget Document Uploads

$ 78,888.00 Requested

Submitted: 8/7/2025 2:11:20 PM (Pacific)

Project Contact
Mark Stone
stonema@reno.gov
Tel: 775-334-3105

Additional Contacts
phelpsa@reno.gov,hancockb@reno.gov,frandenc@reno.gov

City of Reno

PO Box 1900
Reno, NV 89505
United States

Telephone	775-334-3105
Fax	
Web	reno.gov

Director of Finance
Vicki Van Buren
vanburenv@reno.gov

Pre-Application *top*

1. Is your organization one of the following types of entities?: County, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of government, regional government entity, agency or instrumentality of a local government, rural community, unincorporated town or village, or other public entity, tribe, or authorized tribal organization.
Be advised that state agencies receiving SLCGP funds will have to obtain consent for their project from local jurisdictions. A template for obtaining this consent will be provided.

☑ Yes
□ No

2. All funds granted under the State and Local Cybersecurity Grant Program must focus on managing and reducing systemic cyber risk. Does your project proposal aid in achieving this goal? (If not, the project is not eligible for SLCGP funding).

☑ Yes

□ No

3. In order for your application to be considered, you must attend open meetings to testify in front of the Governor's Cybersecurity Task Force. This is a requirement of the grant. If you do not send representation to the required meetings, your application will not be considered.
Meeting dates are to be determined and will be communicated to SLCGP applicants as soon as the dates are known.

☑ I understand and agree.

4. All procurement is required to be compliant with Nevada Revised Statute (NRS) 333, PURCHASING: STATE and/or NRS 332, PURCHASING: LOCAL GOVERNMENTS. **Per FEMA legal opinion, locals may NOT use NRS 332.115 because it has been determined that NRS 332.115 is less restrictive than 2 C.F.R. Part 200 (see Resources section for further justification). All procurement must be free and open competition. Applicants are also 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. Part 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. Part 200.322. Any sole source procurement must be pre-approved in writing by the Office of Emergency Management (OEM) in advance of the procurement.**
You may view FEMA's written legal opinion on NRS 332.115, along with DEM's procurement policy and FEMA's contract provisions guide, in the "Resource Document" tab.

☑ I understand and agree.

5. Supplanting is prohibited under this grant. Supplanting occurs when a subapplicant reduces their own agency's funds for an activity because federal funds are available (or expected to be available) to fund that same activity.

☑ I attest that funding for this project does not currently exist within our agency's budget

6. Entities applying as a subgrantee must meet a 30% cost share requirement for FY 2025 SLCGP. Please acknowledge your understanding and agreement of this requirement.

☑ I understand and agree.

7. Each jurisdiction must complete its own application. The submitter of the grant application will be the recipient of funds. Without an application, OEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.

☑ I understand and agree.

8. Subrecipients (i.e., agencies receiving this funding through the Nevada Office of Emergency Management) may not use this funding to administer their own subawards.

☑ I understand and agree

Application Questions *top*

1. Is this agency considered a rural area (an area encompassing a population of less than 50,000 people)?
If your agency is not considered a rural area, but your project will support rural communities, select "No" and indicate in your narrative what percentage of your project will directly benefit rural Nevadans.

□ Yes

☑ No

2. There are four (4) objectives for FY 2025 SLCGP. Please select the objective with which your

project most closely aligns.

☐ 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.

3. Please select which of the SLCGP program elements your project addresses.

Projects may align with more than one element.

☑ 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.

☐ 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 CISA. (See Application Question 10 for further details on these services.)

☐ 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, cybersecurity services and programs by rural areas within the state.

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

4. Describe your project in detail.

What would you like to do? Why? How does this project improve cybersecurity protection for your agency?

The tool is an additional add-on to our existing endpoint security XDR and SOC services by adding AI behavior baselining and blocking. It's specifically designed to reduce the risk of LOLBins and actions that many cybersecurity systems struggle to tell apart as malicious or day to day IT staff functions.

The tool does this by learning which LOLBins are used regularly, and which aren't for each user account on a given machine. In the event a domain admin or other privileged account is breached attempts to use that access to run mass PowerShell, CMD, WMI, etc, where it has never been done before, will result in the actions being blocked.

This enables IT staff to maintain their domain admin access while adhering to best practices of least privilege. Even with admin access, any actions deviating from baseline behaviors will be blocked.

The rollout will be accomplished by adding the additional license module to our platform. Policies for the specific module will be deployed across the device fleet in waves to ensure minnmal impact and proper testing. The speed of deployment for the platform to learn each user's behvavior should take 30 days or less as it will also build automatic block and allow policies based on EDR logs that are already present for each device.

5. How does your project align with the objective selected in Question 2?

Certain staff and service accounts in the network requiring having higher levels of access to the domain in order to perform their daily duties. However most of the processes software and staff do is very narrow in scope and may only require a few admin level abilities but having admin access grants complete control. Manually build multiple different policies and the changing of the restrictions for those accounts become a constant management headache and opens a window for human error.

By allowing AI and ML to dynamically apply these security restrictions and adjust over time and new job roles and behaviors are learned, the system will constantly adjust to allow for only as needed access and deny all other functions.

This meets Objective 3 because this tool is a major security protection benefit that significantly reduces risk.

6. How does your project align with the program element(s) selected in Question 3?

1. Requested item directly tracks all accounts across all systems especially legacy and end of life platforms and restricts from doing anything else than their core design.

2. Tracks all accounts and their network traffic and will report when they attempted to do something outside of the baseline that was blocked to potentially tip us off sooner if there is an intrusion.

3. Allows us to baseline and harden the environment further ahead of an incident so if a hacker is able to get inside of the environment and privlaged credentials are compromised, the blast radius of damage they are able to achieve is vastly diminished.

4. Being AI and ML driven system it will be constantly learning and baselining the environment. In a future release they are planning to extend the protection offered for data uploads to head off exflitration attempts.

5. Cyber best practice is to limit access to a need only basis and this directly accomplishes this.

10. City of Reno host many critical infrastrcuture systems including Washoe 911 CAD system, waste water treatment plant, and other public safety operations where migitating risk to those services is critical.

7. Does your project address any of the following Key Cybersecurity Best Practices?

☐ Implement multi-factor authentication.
☑ Implement enhanced logging.
☐ Data encryption for data at rest and in transit.
☑ End use of unsupported/end of life software and hardware that are accessible from the internet.
☑ Prohibit use of known/fixed/default passwords and credentials.
☐ Ensure the ability to reconstitute systems (backups).
☐ Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.
☐ Migration to the .gov internet domain.

8. Describe, in detail, how, and by whom, the proposed project will be implemented.

Describe the process by which the project will be accomplished. Identify who (i.e., staff, contractor) will perform the work.

Implementation will be done by the Senior Cybersecurity Analyst, the current admin, and knowledge expert of our EDR/XDR platform that this addition will extend.

9. Describe, in a few sentences, the desired outcome(s) of your project.

The risk of LOLBins both installed by IT as well as built into every default install of Windows Desktop and Server will be nearly eliminated. The platform will allow us to see targeted attemps to run potentially risky scripts and utilities built into Windows and investigate quicker which credentials may be comproised and remediate them before a foothold is established.

10. FY 2025 SLCGP grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities. (This prohibition does not include minor building modifications necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building). For a full list of unallowable costs, please refer to Section D.13 of the FY 2025 SLCGP NOFO.

Please indicate your understanding of this policy.

☑ I understand and agree

11. REQUIRED SERVICES AND MEMBERSHIPS: All SLCGP recipients and subrecipients are required to participate in a limited number of free services by the Cybersecurity and Infrastructure Security Agency (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. --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: https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services. --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) https://www.cisecurity.org/ms-isac/services/ncsr (cisecurity.org).

- ☑ Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR)
- □ Our agency has not yet signed up for the Cyber Hygiene Services or Nationwide Cybersecurity Review (NCSR), but understands we will be required to sign up for them if our project is awarded

12. Provide the 5-digit zip code where the project will be executed.

The project location could be different than the sub-recipient address.

89501

13. Is this project scaleable? Can any part of it be reduced or expanded? Describe the ways in which the project can be reduced or expanded, or the reasons why it cannot.

Yes to an extent. Reducing or expaanding the grant will determine the amount of time that the software license will remain valid for.

14. Is this project shareable or deployable to other jurisdictions?

Select "Yes" if the project supports multiple jurisdictions (e.g., multiple cities). Select "No" if the project primarily supports a single entity.

- □ Yes
- ☑ No

15. Build or Sustain: Select "build" if this project focuses on starting a new capability, or the intent of the project is to close a capability gap. Select "sustain" if the project strictly maintains a core capability at its existing/current level.

- ☑ Build
- □ Sustain

16. If this project is sustaining a previously awarded SLCGP project, please provide the fiscal year and project name of the original project.

N/A

17. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.

- □ Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
- □ Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
- ☑ Equipment - Equipment, supplies, and systems that comply with relevant standards
- □ Training - Content and methods of delivery that comply with relevant training standards
- □ Exercises - Hands-on activities which enhance knowledge of plans, allow members to improve their own performance, and identify opportunities to improve capabilities to respond to real events

Category Budget Totals *top*

Category Budget Breakdown	Costs
Planning	
Organization	
Equipment	$ 78,888.00
Training	
Exercise	
M & A	

Total	**$ 78,888.00**

Line Item Detail Budget *top*

Line Item Detail

List Items (according to POETE categories)	Detailed Description	Quantity	Unit Cost	Total
PLANNING				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
PLANNING Subtotal		**0**	**$ 0.00**	**$ 0.00**
ORGANIZATION				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
ORGANIZATION Subtotal		**0**	**$ 0.00**	**$ 0.00**
EQUIPMENT				
XDR AI Behavior Monitoring and Blocking	Software license module to extend our existing XDR/EDR platform to also cover risky behaviors and LOLBins	1	$ 78,888.00	$ 78,888.00

	and targeted blocking of their use.			
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
EQUIPMENT Subtotal		**1**	**$ 78,888.00**	**$ 78,888.00**
TRAINING				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
TRAINING Subtotal		**0**	**$ 0.00**	**$ 0.00**
EXERCISE				
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00
			$	$ 0.00

EXERCISE Subtotal	**0**	**$ 0.00**	$ 0.00
MANAGEMENT AND ADMINISTRATION			
		$	$ 0.00
		$	$ 0.00
Total	**1**	**$ 78,888.00**	$78,888.00

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	A-133 Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy Purchase Policy
Milestones	☑	Milestones

** ZoomGrants™ is not responsible for the content of uploaded documents.*

Application ID: 506167

Become a fan of ZoomGrants™ on Facebook
Problems? Contact us at Questions@ZoomGrants.com

Logout | Browser