Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Carson City Fire/Emergency Management/Sheriff

Carson City EM / Physical Security Proximity/Camera

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

$ 181,942.00 Requested

Submitted: 8/30/2023 5:22:51 PM (Pacific)

Project Contact
Carson City Fire/Sheriff
carsonfiregrants@carson.org
Tel: 7752837820

Additional Contacts
sduarte@carson.org, fabella@carson.org

Carson City Fire/Emergency Management/Sheriff

777 S. Stewart Street
Carson City, NV 89701
United States

Business Manager
Marty Elzy
MElzy@carson.org

Telephone	7752837820
Fax	
Web	
EIN	88-600189
UEI	DTBPJMA2QFC8
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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 Question 12 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?
Carson City is in the process of designing a new IT Center and an Emergency Operations Center (EOC). The new EM and IT-Cyber facility will require the highest security to keep access to information and hardware restricted to support the city and all of its operations. Not having this support would jeopardize our ability to detect, prevent, and respond to EM and IT-Cyber activities. We are looking to invest into a new state-of-art proximity card, cypher locks, and video camera system to enhance access and security to the centers. We currently do not have badge/card access for the doors and implementing this project will help us to eliminate the use of keys in our environment. This will serve to significantly increase our capacity as it pertains to physical security relative to IT/cyber and the EOC.
This project would include the new system (purchasing of software licensing) and adding proximity readers for doors/gates and video security inside and outside the building. This project helps us to better manage, monitor, and track our badge access system by being able to tell who is access which doors and when.
Additionally, Cypher locks will be purchased and placed on high security areas for dual authentication for access.

5. How does your project align with the objective selected in Question 2?
The implementation of security to the site of both the IT/Cyber Department and the Fire/Emergency Managment Department is essential to buying down risk to the city preparedness, response, and recovery of the two departments responsible for reducing the risk of cyber events in the community. The physical security measures will assist in preventing unwanted access on a critical infrastructure site in the Nevada Capitol and allow for a continuity of government and operations for Carson City.

6. How does your project align with the program element(s) selected in Question 3?
The ability of Carson City to manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the local government within the state, and the information technology deployed on those information systems is imperative to Carson City and the State of Nevada. Ensuring that the local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity by adding physical security to the IT/Cyber Department and the Fire/Emergency Managment will promote continuity of government and operations before, during, and after attempted cyber events.

7. 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.
Installing of all hardware (proximity readers, video cameras, cypher locks, communication boards, and electrical wiring) will be implemented by a vendor. As doors readers are installed by the Vendor, the IT/Cyber Department will monitor the process and approve the installation. IT/Cyber will also monitor, track, investigate, and report any unauthorized attempts to access the centers.

After installation and warranty period are over, the Carson City general fund will be responsible for the ongoing maintenance of the systems.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome of this project is to secure the IT/Cyber and Emergency Managment centers and increase our ability to monitor and track door access. The combination of proximity cards, cypher locks, and video camera systems will ensure a more restricted access and monitoring of permitted physical access. These systems allow us the ability to set alerts when specific badges/doors are used, increasing our ability to track those attempting access to secure rooms.
Ensures continuity of IT 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.
This project will prevent, assess and mitigate, to the greatest degree possible, cybersecurity risks and threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within Carson City.
Enhance capabilities to share physical threat indicators of a municipality and related information between the local, state, and CISA partners.
Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
Implement an IT and physical technology modernization review process that ensures alignment between information technology and operational technology cybersecurity objectives.
Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
N/A

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.

- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☐ 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. 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. Should there not be enough funding from the state, Carson City could implement in phases across several CISA Cyber Security Grant cycles to procure, install, and make operational. The combination of three types of physical security and the three phases of operational completion would allow for scalability.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89701

14. 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.
- [x] Build
- [ ] Sustain

15. 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.
- [x] Yes
- [ ] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [ ] Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
- [x] Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	**$ 0.00**	**$ 0.00**		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Intrusion Security System, Infrastructure Only	System wiring project for	18,024	$ 1.75	$ 31,542.00	Hardware required to support the	After initial install, the maintenance	System, Intrusion Detecti	05NP-00-IDPS

	the entire system by square feet				product/service.	would be general fund		
Access Control System, Keypad/Controller	6 panels, one in each external access of the building	6	$ 5,000.00	$ 30,000.00	Hardware required to support the product/service.	After initial install, the maintenance would be general fund	System, Intrusion Detecti	05NP-00-IDPS
Cypher locks	15 high security point cyphers	15	$ 2,000.00	$ 30,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	System, Intrusion Detecti	05NP-00-IDPS
Multi-Directional Sensor Camera	10 Multi-Directional Sensor Cameras for intrusion tracking	10	$ 1,900.00	$ 19,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	Systems, Video Assessment	14SW-01-VIDA
Fish Eye Camera	10 Fish Eye Cameras	10	$ 900.00	$ 9,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	Systems, Video Assessment	14SW-01-VIDA
Standard Camera	6 Standard Surveillance Cameras	6	$ 400.00	$ 2,400.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	Systems, Video Assessment	14SW-01-VIDA
Access Control Proximity Strike pad	20 Proximity Strike pads	20	$ 1,000.00	$ 20,000.00	Hardware required to support the product/service.	It would be cut from budget if not funded. Maintenance would be general fund.	System, Credentialing	4AP-05- CRED
Vendor installation	Contractor will install the hardware and software for physical security.	1	$ 40,000.00	$ 40,000.00	The Vendor will install the proximity access, Cypher locks, and video camera security systems.	The program would have to be reduced for initial project development. The ongoing maintenance will be budgeted for in the city general fund.		
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		18,092	**$ 51,201.75**	**$ 181,942.00**				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	**$ 0.00**			**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		0
Total		0	$ 0.00	$0.00		0

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	CC Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Compensation Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestone Carson City 2023
		Carson City Capabilities Assessment 2023
		CC Fire Capabilities

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

Application ID: 449130

List project milestones and anticipated completion dates which can be used to determine success at each phase of the project.

	Applicant Name	Carson City Fire/EM
	Project Name:	EOC Proximity Access and Video
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Receive award notification	12/31/23
2	Bid process for Vendors	6/1/24
3	Purchase Equipment	9/1/23
4	Install Equipment	1/31/25
5	Pay PO and Seek reimbursement	3/31/25
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

Outlook

Re: Determination of allowability for Carson City Emergency Management's Physical Security Proximity/Camera project

From Jon Bakkedahl <JBakkedahl@carson.org>
Date Thu 10/03/24 5:03 PM
To Amanda Jackson <amanda.jackson@dem.nv.gov>; Carson Fire Grants <carsonfiregrants@carson.org>; Frank Abella <FAbella@carson.org>; Dave Aurand <DAurand@carson.org>
Cc Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Susan Coyote <scoyote@dem.nv.gov>; Zachary R. Edler <zedler@dem.nv.gov>; Keri M. Beach <Keri.Beach@dem.nv.gov>

Thank you for the opportunity to re-submit, knowing it still may not be allowed.
V/R;

Jon Bakkedahl, MS, CEM, NVEM
Deputy Emergency Manager
Carson City Fire Department
P:775-283-7820 | **C**:775-722-9760
jbakkedahl@carson.org | www.carsonfire.org
777 S. Stewart St. Carson City, NV 89701
AMBASSADOR™ WRN WEATHER-READY NATION
Office hours: Monday - Thursday 7 am to 5:30 pm

Sign up for Carson City Alerts at !CARSON and get the information you need!

From: Amanda Jackson <amanda.jackson@dem.nv.gov>
Sent: Thursday, October 3, 2024 4:28 PM
To: Jon Bakkedahl <JBakkedahl@carson.org>; Carson Fire Grants <carsonfiregrants@carson.org>; Frank Abella <FAbella@carson.org>; Dave Aurand <DAurand@carson.org>
Cc: Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Susan Coyote <scoyote@dem.nv.gov>; Zachary R. Edler <zedler@dem.nv.gov>; Keri M. Beach <Keri.Beach@dem.nv.gov>
Subject: Re: Determination of allowability for Carson City Emergency Management's Physical Security Proximity/Camera project

---

Hi Jon,

As a follow-up to our conversation, I wanted to send you the guidance from FEMA that came out about SLCGP. Please see the highlighted portion on page 30 of the attached document. In two of the last FY 2024 SLCGP webinars, FEMA said this policy will apply retroactively to FY 2022 and FY 2023.

What exactly is considered "minor building modifications necessary to install and connect grant-purchased equipment" is not clear, but FEMA said they will be releasing an information bulletin in the coming weeks to offer clarification. The question about physical security cameras was asked specifically in both webinars this week, so I am hopeful they will address that directly.

The Governor's Cybersecurity Task Force ranking and voting meeting to allocate the remaining FY 2023 SLCGP funds is Monday, October 14, at 12:30pm. I am not sure if the FEMA information bulletin will be out before the ranking and voting meeting, but if it turns out that FEMA will allow even some portion of this project, I want to make sure Carson City has a shot at that.

I will make sure you have the link for the meeting so you can once again speak on your project, and I will attach this email to the meeting materials for the task force so they are aware of why they're seeing this project again.

Please let me know if you have any questions!

Amanda Jackson
Grants & Projects Analyst II, Southern Nevada
Office Hours: Mon-Fri, 7:00am-4:00pm

Nevada Division of Emergency Management / Homeland Security
Prevent • Protect • Mitigate • Respond • Recover

4500 W Silverado Ranch Blvd
Las Vegas, NV 89139
775-546-8055
775-687-0498 - 24/7/365 Emergency Duty

Book time to meet with me

Make sure you receive all DEM grants communication! Email DHSgrants@dem.nv.gov to be added to the grants listserv.

http://dem.nv.gov

From: Zachary R. Edler <zedler@dem.nv.gov>
Sent: Wednesday, December 27, 2023 9:54 AM
To: jbakkedahl@carson.org <jbakkedahl@carson.org>; Amanda Jackson <amanda.jackson@dem.nv.gov>; Carson Fire Grants <carsonfiregrants@carson.org>; Frank Abella <FAbella@carson.org>; Dave Aurand <DAurand@carson.org>
Cc: Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Jared L. Franco <jaredfranco@dem.nv.gov>; Susan Coyote <scoyote@dem.nv.gov>; David W. Fogerson <dfogerson@dem.nv.gov>
Subject: RE: Determination of allowability for Carson City Emergency Management's Physical Security Proximity/Camera project

Good morning, Jon,

Thank you for your questions.

The grant funds will be considered deobligated for purposes of the program. Because of that, funding will move down to the next approved project below the red line for funding.

Carson City can absolutely apply for other funding through the program, but it would be out of deobligated funds in the future.

We do not currently have a timeline for these funds. Since the program doesn't have awards made yet we don't have the data available to understand how quickly the funds will be spent by other applicants.

I'm happy to schedule a call with you to discuss any of this or any other questions you may have.

Thank you,
Zachary Edler

Recurring Grants Supervisor

Nevada Division of Emergency Management / Homeland Security

Prevent • Protect • Mitigate • Respond • Recover

2478 Fairview Dr, Carson City, NV 89701
Office 775-687-0373
zedler@dem.nv.gov
6:30 to 5:30 Monday – Wednesday & Friday
Off Thursdays
dem.nv.gov

Visit [www.ready.gov]www.ready.gov to learn how to be prepared for an emergency.

From: Jon Bakkedahl <JBakkedahl@carson.org>
Sent: Wednesday, December 27, 2023 9:10 AM
To: Amanda Jackson <amanda.jackson@dem.nv.gov>; Carson Fire Grants <carsonfiregrants@carson.org>; Frank Abella <FAbella@carson.org>; Dave Aurand <DAurand@carson.org>
Cc: Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Jared L. Franco <jaredfranco@dem.nv.gov>; Susan Coyote <scoyote@dem.nv.gov>; Zachary R. Edler <zedler@dem.nv.gov>; David W. Fogerson <dfogerson@dem.nv.gov>
Subject: Re: Determination of allowability for Carson City Emergency Management's Physical Security Proximity/Camera project

Good morning,
Thank you for the correspondence, we have three questions:

1. What happens to the voted on and approved funding?
2. Will Carson City have to re-apply or change our application?
3. What will be the timeframe?

According to the attached emails, there is an opportunity for Carson City to apply for funding in the same building as stated here for tabletop equipment in the EOC and IT Center:

ALLOWABLE COSTS
For costs to be allowable they must align with 2 CFR Part 200 Cost Principles Sub Part E, the DHS Terms and Conditions, and the SLCGP goals and objectives. Examples of types of allowable costs include the following:
Replacing or installing servers, communication, or network components onto existing racks and using existing cabling
Installation of new equipment cabling through existing conduit and no new holes in walls, ceilings, or floors
Tabletop equipment such as computers, monitors, and workstations
Software

V/R;

Jon Bakkedahl, MS, CEM, NVEM
Deputy Emergency Manager
Carson City Fire Department
P:775-283-7820 | **C**:775-722-9760
jbakkedahl@carson.org | www.carsonfire.org
777 S. Stewart St. Carson City, NV 89701
AMBASSADOR™ WEATHER-READY NATION
Office hours: Monday - Thursday 7 am to 5:30 pm

From: Amanda Jackson <amanda.jackson@dem.nv.gov>
Sent: Tuesday, December 26, 2023 1:11 PM
To: Carson Fire Grants <carsonfiregrants@carson.org>; Frank Abella <FAbella@carson.org>; Dave Aurand <DAurand@carson.org>; Jon Bakkedahl <JBakkedahl@carson.org>; Serge Duarte <SDuarte@carson.org>
Cc: Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Jared L. Franco <jaredfranco@dem.nv.gov>; Susan Coyote <scoyote@dem.nv.gov>; Zachary R. Edler <zedler@dem.nv.gov>

Subject: Determination of allowability for Carson City Emergency Management's Physical Security Proximity/Camera project

---

Good afternoon,

I am writing to inform you of clarification we received from FEMA regarding the FY 2023 State and Local Cybersecurity Grant Program (SLCGP) Notice of Funding Opportunity (NOFO) and allowable projects.

Section F.3, Administrative and National Policy Requirements, Part c., of the FY 2023 SLCGP NOFO does discuss the Environmental and Historic Preservation Review process for projects which may disturb buildings or grounds, however, Section D.13, Funding Restrictions and Allowable Costs, states that, *"...For FY 2023 SLCGP, grant funds may not be used: ...To acquire land or to construct, remodel, or perform alternations of buildings or other physical facilities."* The attached email from FEMA provides clarification on these sections and the federal definition of "construction," "remodel," and "alterations of buildings." In light of this clarification, it has been determined that Carson City Emergency Management's Physical Security Proximity/Camera project is unallowable under FY 2023 SLCGP.

I am happy to meet with you at any time if you would like to discuss this further, and I apologize for the confusion and trouble this determination may cause. I invite you to resubmit this project during the next Homeland Security Grant Program (HSGP) application period, as HSGP is specifically geared toward physical security projects, does allow for modifications to structures, and may be a more appropriate source of funding.

Thank you,

Amanda Jackson
Grants & Projects Analyst II, Southern Nevada
Office Hours: Mon-Fri, 7:00am-4:00pm

Nevada Division of Emergency Management / Homeland Security
Prevent • Protect • Mitigate • Respond • Recover

4500 W Silverado Ranch Blvd
Las Vegas, NV 89139
775-546-8055
775-687-0498 - 24/7/365 Emergency Duty

Make sure you receive all DEM grants communication! Email DHSgrants@dem.nv.gov to be added to the grants listserv.

http://dem.nv.gov

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

City of Caliente
MFA on Desktop

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

$ 10,550.00 Requested

Submitted: 9/20/2024 1:55:45 PM (Pacific)

Project Contact
Joseph Lamb
jlamb@cityofcaliente.com
Tel: 7759623275

Additional Contacts
none entered

City of Caliente

100 Depot Avenue
Caliente, NV 89008
United States

City Manager
Craig Roisum
croisum@cityofcaliente.com

Telephone	7757263131
Fax	
Web	cityofcaliente.com
EIN	88-6000186
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 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.

- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 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.
- [x] 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?
Implementing Multi-Factor Authentication (MFA) can significantly enhance cybersecurity protection for the City of Caliente in several ways:

1. Enhanced Security: MFA adds an extra layer of security by requiring users to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN. This makes it much harder for attackers to gain access, even if they have compromised one factor (like a password).

2. Reduced Risk of Credential Theft: With MFA, even if an attacker manages to steal a user's password, they would still need the second factor (such as a mobile device or biometric verification) to access the account. This greatly reduces the risk of unauthorized access.

3. Protection Against Phishing: MFA can help protect against phishing attacks. Even if a user inadvertently provides their credentials to a phishing site, the attacker will still need the second factor to complete the login process.

4. Compliance with Regulations: Many regulatory frameworks and standards, such as GDPR, HIPAA, and NIST, recommend or require the use of MFA to protect sensitive data. Implementing MFA can help your agency stay compliant with these regulations.

5. User Awareness and Training: Implementing MFA often comes with increased user awareness and training about cybersecurity best practices, which can further enhance overall security posture.

6. Flexibility and Scalability: Modern MFA solutions are flexible and can be scaled to fit the needs of any organization, from small agencies to large enterprises. They can be integrated with various systems and applications, providing comprehensive protection across the board.

5. How does your project align with the objective selected in Question 2?
Multi-Factor Authentication (MFA) implements security protections that are commensurate with risk by tailoring the level of security to the sensitivity of the data and the potential impact of a security breach. Here's how it achieves this:

1. Risk-Based Authentication: MFA systems can adjust the authentication requirements based on the risk level of the login attempt. For example, if a login attempt is made from an unusual location or device, the system can require additional verification steps.

2. Granular Access Control: MFA allows for more granular access control, ensuring that only authorized users can access sensitive information. This is particularly important for protecting high-value assets and critical systems.

3. Adaptive Authentication: Some MFA solutions use adaptive authentication, which assesses the risk of each login attempt in real-time. Factors such as user behavior, device health, and network security are analyzed to determine the appropriate level of authentication required.

4. Compliance with Security Policies: MFA helps organizations comply with internal security policies and external regulations that mandate strong authentication measures for accessing sensitive data.

5. Mitigation of Credential-Based Attacks: By requiring multiple forms of verification, MFA significantly reduces the risk of credential-based attacks, such as phishing, brute force attacks, and credential stuffing.

6. User Education and Awareness: Implementing MFA often involves educating users about the importance of security and the risks associated with their actions. This increased awareness can lead to better security practices overall.

By aligning the level of authentication with the risk associated with the access request, MFA ensures that security measures are appropriately scaled to protect against potential threats.

6. How does your project align with the program element(s) selected in Question 3?
Managing, Monitoring, and Tracking

1. Enhanced Security: MFA requires multiple forms of verification, making it difficult for unauthorized users to access systems, even if they have compromised one form of authentication.
2. Protection Against Phishing and Credential Theft: By requiring additional authentication factors, MFA reduces the risk of account takeovers from phishing attacks or stolen credentials.
3. Monitoring and Tracking: MFA can be integrated with monitoring tools to track login attempts and identify suspicious activities, aiding in quick detection and response to potential security breaches.
4. Access Control: Ensures only authorized personnel can access sensitive information and systems, crucial for managing legacy systems with outdated security measures.

5. Compliance and Accountability: Helps meet regulatory requirements and provides an audit trail of access attempts, useful for compliance and accountability.
6. Support for Legacy Systems: Adds an additional layer of security to legacy systems, mitigating risks associated with outdated technology.

Enhancing Preparation, Response, and Resilience

1. Preparation: MFA strengthens the initial security posture by ensuring that only verified users can access critical systems and data. This preparation is crucial for defending against potential cyber threats.
2. Response: In the event of a security incident, MFA helps contain the breach by preventing unauthorized access to other parts of the network. This limits the spread of the attack and allows for a more effective response.
3. Resilience: MFA contributes to the overall resilience of information systems by providing an additional layer of defense. Even if one security measure fails, MFA ensures that there are other barriers in place to protect against unauthorized access.
4. Phishing-Resistant: MFA, especially phishing-resistant methods, significantly reduces the likelihood of successful phishing attacks, which are common entry points for cyber threats.
5. Continuous Improvement: By integrating MFA with other security measures, state and local governments can continuously improve their cybersecurity posture, adapting to new threats and vulnerabilities as they arise.

By implementing MFA, the city better manage and secure their information systems while also enhancing their ability to prepare for, respond to, and recover from cybersecurity threats. This dual approach ensures a robust defense against a wide range of cyber risks.

7. 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.
An on-stie contractor that is currently working with the City of Caliente will help draft SOW (Statement of Work) and implement a solution with Subject Matter Expert (SME). The SME will be a remote engineer from the 3rd party vendor providing the service.

8. Describe, in a few sentences, the desired outcome(s) of your project.
All users will need MFA to authenticate and use City's resources and data. The City's personal information will be protected with another level of protection.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- [ ] Yes
- [x] No

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), either on our own or as a condition of FY 2022 SLCGP
- [x] 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. 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.
This project is scalable to all department in the City of Caliente.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89008

14. 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.
- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [ ] 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
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	0.00	$ 0.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
MFA Vendor	MFA	1	$ 8,000.00	$ 8,000.00	This is the main item for this project.	The city will have to pay for the Firewall if the grant funding was reduced. MFA is essential to doing business now.		
Installation Cost		10	$ 180.00	$ 1,800.00	This will pay for the contractor to install the project.	After the installation, the city will pay for the contractor to maintain the system.		
Cryptokeys	Key	15	$ 50.00	$ 750.00	This key will store users One time Password number used in the MFA process.	The key could be generated on users smart phone, but not all users will allow the cell for City's usage.	System, Remote Authentic	05AU-00-TOKN
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				

			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		26	$ 8,230.00	$ 10,550.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

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

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

Application ID: 481958

	Applicant Name	City Of Caliente
	Project Name:	MFA
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Grant Writing and Approval	15-Oct
2	**Project Planning**:	15-Nov
3	**Vendor Selection**	1-Dec
4	**Preparation:**	10-Dec
5	**Hardware and Software Procurement**	31-Dec
6	**Configuration and Setup**	15-Jan
7	**Training and Documentation**	20-Jan
8	**Implementation and Go-Live**	1-Feb
9	**Monitoring and Maintenance**	15-Feb
10	Project Review and Closure	1-Mar

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

City of Caliente

NIST CSF v2.0 Gap Analysis

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

$ 22,500.00 Requested

Submitted: 9/24/2024 6:53:42 PM (Pacific)

Project Contact
Joseph Lamb
jlamb@cityofcaliente.com
Tel: 7759623275

Additional Contacts
none entered

City of Caliente

100 Depot Avenue
Caliente, NV 89008
United States

City Manager
Craig Roisum
croisum@cityofcaliente.com

Telephone	7757263131
Fax	
Web	cityofcaliente.com
EIN	88-6000186
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 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 Question 12 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 primary objective of this engagement is to conduct a thorough and nuanced gap analysis aimed at evaluating the current cybersecurity posture of the City in relation to the standards set forth by the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF V2).

Unlike traditional audit processes that often rely on a checklist
approach to identify compliance gaps, this engagement is designed to be much more dynamic and contextual. It leverages the expertise of a seasoned Chief Information Security Officer (CISO) with extensive governance and technical background. This approach ensures that the analysis and subsequent recommendations are not only aligned with the NIST CSF V2 but also tailored to the unique needs, priorities, and realities of City's business. The ultimate goal is to provide the city with a clear and actionable roadmap that not only highlights areas of non-compliance but also offers prioritized, realistic,
and contextually relevant strategies for improvement, thereby enhancing the overall security posture and compliance with the NIST CSF V2.

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

Performing a NIST 2.0 cybersecurity assessment can significantly benefit the City in several ways:

1. Adopting Best Practices and Methodologies:
- Standardized Approach: NIST CSF 2.0 provides a standardized framework that helps organizations adopt best practices and methodologies for cybersecurity. This ensures consistency and comprehensiveness in addressing cybersecurity risks.
- Guidance and Resources: The framework links to various resources and guidelines that help organizations implement effective cybersecurity measures.

2. Enhancing Preparation, Response, and Resilience:
- Risk Management: NIST CSF 2.0 helps organizations identify, assess, and manage cybersecurity risks more effectively. This proactive approach enhances their ability to prepare for potential threats.
- Incident Response: The framework emphasizes the importance of detecting, responding to, and recovering from cybersecurity incidents. This ensures that state and local governments can quickly address and mitigate the impact of cyber threats.
- Continuous Improvement: By defining clear metrics and performance indicators, NIST CSF 2.0 facilitates continuous improvement in cybersecurity practices. This ongoing process helps organizations stay resilient against evolving threats.

Overall, adopting NIST CSF 2.0 helps the City create a robust cybersecurity posture, ensuring they are well-prepared to handle cybersecurity risks and threats effectively.

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

Using the NIST Cybersecurity Framework (CSF) 2.0 to understand the City's current cybersecurity posture and identify areas for improvement involves several key steps:

1. Establish a Baseline:
- Current Profile: Start by creating a Current Profile that documents our organization's existing cybersecurity practices and controls. This helps in understanding where the City currently stands.

2. Conduct Risk Assessments:
- Identify Risks: Use the framework to identify and assess cybersecurity risks. This involves evaluating potential threats and vulnerabilities that could impact your information systems.
- Prioritize Risks: Rank the identified risks based on their potential impact and likelihood. This helps in focusing on the most critical areas first.

3. Continuous Testing and Evaluation:

- Regular Assessments: Perform regular assessments to test the effectiveness of your cybersecurity measures. This includes vulnerability assessments, penetration testing, and security audits.
- Metrics and KPIs: Define and track key performance indicators (KPIs) and metrics to measure the City' cybersecurity posture over time.

4. Structured Assessments:
- Gap Analysis: Conduct a gap analysis to compare your Current Profile with the desired Target Profile. This helps in identifying areas where improvements are needed.
- Action Plans: Develop action plans to address the gaps identified. This includes implementing new controls, enhancing existing ones, and continuously monitoring progress.

5. Continuous Improvement:
- Feedback Loop: Establish a feedback loop to continuously improve your cybersecurity practices. This involves regularly reviewing and updating your profiles, risk assessments, and action plans based on new threats and changes in the environment.

By following these steps, The City can use the NIST CSF 2.0 to gain a comprehensive understanding of your cybersecurity posture and continuously improve its defenses against evolving threats.

7. 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.
Scope of Work: The work will be done with City's personnel and Cybersecurity Consultant

1. Initial Consultation and Data Collection:
Objective: To establish a comprehensive baseline of Client's current cybersecurity landscape and practices within the organization.
Activities:
o Collection and review of existing cybersecurity policies, procedures, and documentation by city and consultant.
o Assessment of the current security architecture, technologies in use, and any existing compliance reports or audits by consultant.
o Identification of critical assets, data flows, and protection mechanisms currently in place by city personnel.

2. Interviews with Key Personnel: (all by consultant)
Objective: To gain in-depth insights into the operational, tactical, and strategic aspects of Client's cybersecurity efforts.
Activities:
o Conducting structured interviews with IT staff, security officers, executive management, and other relevant stakeholders.
o Discussions to understand the perceived versus actual security needs, concerns, and expectations from various departments.
o Gathering qualitative data on security culture, awareness, and stakeholder engagement in cybersecurity initiatives.

3. Technical and Process Evaluation: (by consultant)
Objective: To critically assess the alignment of Client's technical and procedural controls with the NIST CSF V2.
Activities:
o Evaluation of the effectiveness and coverage of current cybersecurity measures against the NIST CSF
V2 categories and subcategories.
o Assessment of the integration of cybersecurity practices into Client's daily operations and decision making processes.
o Identification of strengths, weaknesses, and potential areas for improvement in Client's cybersecurity framework.

4. Gap Analysis Execution: (Consultant)
Objective: To systematically identify and document gaps in compliance with the NIST CSF V2, prioritizing findings based on risk, impact, and business context.
Activities:
o Utilization of a detailed checklist aligned with NIST CSF V2 controls to methodically identify non compliance areas.
o Analysis of gaps to determine underlying causes, potential risks, and the impact on Client's security posture.
o Development of a prioritized list of recommendations for addressing identified gaps, taking into consideration Client's business objectives, resources, and risk tolerance.

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

A Comprehensive Gap Analysis Report: Documenting current compliance levels, identified gaps, and contextual analysis of the cybersecurity posture against the NIST CSF V2.

Actionable Roadmap: A prioritized and realistic plan detailing steps to achieve and maintain compliance with the NIST CSF V2, including short-term fixes and long-term strategic initiatives.

Enhanced Cybersecurity Posture: Through the implementation of the roadmap, Client will strengthen its defenses, reduce risk, and align more closely with NIST CSF V2 requirements, thereby enhancing its overall security and resilience against cyber threats.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP

- [x] 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. 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.
We can reduce the number of items in the NIST framework covered.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89008

14. 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.
- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
NIST Assement	NIST 2.0 Assessment	1	$ 18,900.00	$ 18,900.00	This is the main item for this project. The assessment will set cybersecurity goals for the next few years.	This is a great opportunity to have skilled auditor look at our systems. This could not be achieved easily with the City paying for it.
Remediation	Local contractor efforts to apply the assessment results	20	180.00	$ 3,600.00	This will pay for the city to help remediate the issues found after the vendor completed the assessment.	After the installation, the city will pay for a contractor to maintain the system.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		21	**$ 19,080.00**	**$ 22,500.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$	
		0	$ 0.00	$ 0.00	

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		0	$ 0.00	$ 0.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

	0	$ 0.00	$ 0.00		0
Total	**0**	**$ 0.00**	$0.00		**0**

Document Uploads *top*

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

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

Application ID: 482799

	Applicant Name	City Of Caliente
	Project Name:	NIST Assesment
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Grant Writing and Approval	15-Oct
2	**Project Planning**:	15-Nov
3	**Vendor Selection**	1-Dec
4	**Prepare for the Assessment**:	10-Dec
5	**Conduct the Assessment:**	31-Dec
6	**Monitoring and Maintenance**	15-Jan
7		
8		
9		
10	Project Review and Closure	1-Mar

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

City of Caliente
SEIM Tool

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

$ 37,800.00 Requested

Submitted: 9/20/2024 1:51:31 PM (Pacific)

Project Contact
Joseph Lamb
jlamb@cityofcaliente.com
Tel: 7759623275

Additional Contacts
none entered

City of Caliente

100 Depot Avenue
Caliente, NV 89008
United States

City Manager
Craig Roisum
croisum@cityofcaliente.com

Telephone	7757263131
Fax	
Web	cityofcaliente.com
EIN	88-6000186
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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 Question 12 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.
- [x] 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 City needs a security monitoring and log management platform or SEIM. This tool should include network visibility, host visibility, intrusion detection honeypots, log management, and case management.

A Security Information and Event Management (SIEM) system is a cybersecurity solution that helps organizations detect, analyze, and respond to security threats in real-time. SIEM systems combine two key functions:

1. Security Information Management (SIM): This involves collecting and managing security-related data from various sources.
2. Security Event Management (SEM): This focuses on analyzing and responding to security events and incidents.

By integrating these functions, SIEM systems provide a centralized view of an organization's security posture, enabling quick detection and response to potential threats. They are essential for meeting compliance requirements and improving overall security operations.

This tool will help in the following ways:
Threat Hunting and Log Management Tool (SEIM) protects businesses through a multi-layered approach to cybersecurity, integrating various tools and techniques to provide comprehensive security monitoring and threat detection. Here are some key ways it helps:
1. Intrusion Detection: SEIMs uses tools like Suricata and Zeek to monitor network traffic for suspicious activity and potential threats1.
2. Log Management: It centralizes and analyzes logs from various sources, making it easier to detect anomalies and investigate incidents2.
3. Threat Hunting: The platform includes tools for proactive threat hunting, allowing security teams to search for indicators of compromise (IoCs) and other signs of malicious activity2.
4. Full Packet Capture: SEIMs can capture and store network traffic, providing detailed data for forensic analysis1.
5. Host Monitoring: SEIM can use the Elastic Agent and osquery to monitor host systems for signs of compromise.
6. User-Friendly Interfaces: The platform offers custom interfaces for alerts, dashboards, and case management, making it easier for security teams to manage and respond to threats.
By integrating these tools and capabilities, SEIMs helps businesses detect, investigate, and respond to cybersecurity threats more effectively, thereby enhancing their overall security posture.

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

SEIMs helps businesses develop and establish appropriate governance structures and cybersecurity plans through several key features and practices:
1. Comprehensive Monitoring and Detection: By integrating tools like Suricata, Zeek, and Elastic Agent, SEIMs provides continuous monitoring and detection of network and host activities. This helps in identifying potential threats and vulnerabilities in real-time1.
2. Centralized Log Management: SEIM centralizes logs from various sources, making it easier to analyze and correlate data. This centralized approach supports the development of effective incident response plans by providing a clear view of the security landscape2.
3. Threat Hunting and Forensics: The platform includes tools for proactive threat hunting and forensic analysis. This allows security teams to investigate incidents thoroughly and develop strategies to prevent future occurrences.
4. Customizable Dashboards and Alerts: SEIM offers customizable dashboards and alerting mechanisms. These features enable organizations to tailor their monitoring and response strategies to their specific needs, ensuring that critical incidents are detected and addressed promptly.
5. Training and Documentation: SEIM provides extensive documentation and training resources. These resources help organizations understand how to implement and use the platform effectively, ensuring that staff are well-prepared to respond to cybersecurity incidents.

By leveraging these features, SEIM helps entities establish robust governance structures and cybersecurity plans, enhancing their ability to respond to incidents and maintain continuity of operations.

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

1. A SEIM will Manage, monitor, and track information systems, applications, and user accounts owned by the City of Caliente.
2. This product will monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned by the City. This product will also be able to create raw network logs for analysis.
3. A SEIM will help in preparation, response, and resilience of information systems, applications, and user accounts owned by the city against cybersecurity risks and cybersecurity threats. A Seim will have alerting (email) capabilities 24 hours 7 days a week.

7. 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.
This project will be implemented by a contractor under the guidance of the vendor. The City does not employ any permeant IT staff.
A SEIM will be a Virtual Machine which will be hosted on the City's Host server. There will need to be a mirror port setup on the switch to capture network traffic. There is also an agent to get all the log files sent to the collector.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The goal is 24/7/365 cybersecurity monitoring without the expense of a SOC (security operations Center)

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- [ ] Yes
- [x] No

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), either on our own or as a condition of FY 2022 SLCGP
- [x] 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. 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.
We can reduce the amount support if needed.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89008

14. 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.
- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [ ] 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
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
SEIM	Log Management Server	1	$ 36,000.00	$ 36,000.00	This is the main item for this project.	This project could purchase a solution based on open-source software. If need be, the City can use the free version. However, the free version is missing features key to security, such as email alerts.	SEIM	05NP-00-SIEM
Installation Cost		10	$ 180.00	$ 1,800.00	This will pay for the contractor to install the project.	After the installation, the city will pay for the contractor to maintain the system.		
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		11	$ 36,180.00	$ 37,800.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	**$0.00**			**0**

Document Uploads *top*

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

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

Application ID: 481358

	Applicant Name	City of Caliente
	Project Name:	SEIM
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Complete Grant Application	27-Sep
2	Define the scope of the SIEM implementation, including the number of data sources, required integrations, and customizations	1-Nov
3	Conduct a thorough assessment of our current security infrastructure and identify gaps	15-Nov
4	Evaluate and select the appropriate SIEM solution that meets the City's needs	1-Dec
5	Install the SIEM software and configure it to collect data from various sources	15-Dec
6	Integrate the SIEM with existing security tools and systems	20-Dec
7	Conduct thorough testing to ensure the SIEM system is functioning correctly	15-Jan
8	Train the security team on how to use the SIEM system effectively	30-Jan
9	Officially launch the SIEM system and begin live monitoring	1-Feb
10	Regularly review and update SIEM rules and configurations to adapt to new threats	5-Feb
11	Complete Grant Project by documentation and closure of funds	15-Feb
12	Post Project Evaluation with Stakeholders	1-Mar

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

City of Caliente
Site-To-Site VPN

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

$ 4,800.00 Requested

Submitted: 9/20/2024 1:59:36 PM (Pacific)

Project Contact
Joseph Lamb
jlamb@cityofcaliente.com
Tel: 7759623275

Additional Contacts
none entered

City of Caliente

100 Depot Avenue
Caliente, NV 89008
United States

City Manager
Craig Roisum
croisum@cityofcaliente.com

Telephone	7757263131
Fax	
Web	cityofcaliente.com
EIN	88-6000186
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 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.
- [x] 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?

Issue: The City Offices and the City Maintenance Department are operating on separate networks. The City Maintenance Department is currently using a home firewall that lacks proper updates and maintenance. Additionally, there is no web filtering system in place for the City Maintenance Shop.

Resolution: Site-To-Site VPN

Site-to-site VPNs offer several cybersecurity benefits, making them a popular choice for organizations with multiple locations. Here are some key advantages:
1. Enhanced Data Security: Site-to-site VPNs use encryption to secure data as it travels between different sites. This ensures that sensitive information remains confidential and protected from unauthorized access.
2. Secure Communication: By creating a secure, encrypted tunnel between networks, site-to-site VPNs prevent data interception and eavesdropping by malicious actors.
3. Simplified Resource Sharing: These VPNs allow for the secure sharing of resources such as file servers and databases across different locations without exposing them directly to the internet.
4. Cost-Effective Network Expansion: Site-to-site VPNs can be a more cost-effective solution compared to traditional private networks, as they leverage existing internet connections to securely connect different sites.
5. Operational Continuity: They support operational continuity by allowing employees to securely access the corporate network from remote locations, reducing potential downtime during emergencies.

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

A site-to-site VPN can significantly enhance the ability to monitor, audit, and track network traffic and activity for state or local government systems in several ways:

1. Unified Network: By connecting the City Offices and the City Maintenance Department into a single, secure network, a site-to-site VPN ensures that all traffic between these locations is encrypted and routed through a central point. This centralization simplifies monitoring and auditing.

2. Enhanced Security: The VPN encrypts data in transit, protecting it from interception and unauthorized access. This encryption ensures that sensitive information remains confidential and secure, which is crucial for government operations.

3. Centralized Monitoring: With a unified network, IT administrators can use centralized tools to monitor and track all network traffic and activities. This centralization allows for more efficient and comprehensive auditing and tracking of user activities, application usage, and data transfers.

4. Compliance and Reporting: A site-to-site VPN can help meet regulatory requirements by providing detailed logs and reports of network activity. These logs can be used for compliance audits and to demonstrate adherence to security policies and regulations.

5. Improved Management: Centralized management of network security policies and updates becomes easier with a site-to-site VPN. IT staff can ensure that all connected sites adhere to the same security standards and receive timely updates and patches.

6. Web Filtering: Implementing a site-to-site VPN allows for the deployment of web filtering solutions at a central point, ensuring that all traffic from the City Maintenance Department is subject to the same web filtering policies as the City Offices.

By integrating these departments into a single, secure network, a site-to-site VPN provides a robust framework for monitoring, auditing, and tracking network activities, thereby enhancing overall security and compliance.

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

A site-to-site VPN can play a crucial role in enhancing the preparation, response, and resilience of information systems, applications, and user accounts against cybersecurity risks and threats in several ways:

1. Secure Communication: By encrypting data transmitted between different sites, a site-to-site VPN ensures that sensitive information remains confidential and protected from interception by malicious actors. This secure communication channel is essential for maintaining the integrity of government operations.

2. Centralized Security Management: A site-to-site VPN allows for centralized management of security policies and updates. IT administrators can enforce consistent security measures across all connected sites, ensuring that all systems are up-to-date with the latest patches and security protocols.

3. Improved Incident Response: With a unified network, IT teams can quickly detect and respond to security incidents. Centralized monitoring tools can provide real-time alerts and detailed logs, enabling faster identification and mitigation of threats.

4. Enhanced Resilience: A site-to-site VPN can improve network resilience by providing redundant connections between sites. In the event of a network failure at one site, traffic can be rerouted through alternative paths, ensuring continuous operation and minimizing downtime.

5. Disaster Recovery: By connecting multiple sites, a site-to-site VPN facilitates robust disaster recovery plans. Data can be securely backed up and replicated across different

locations, ensuring that critical information is preserved and can be quickly restored in case of a cyberattack or other disaster.

6. Access Control: A site-to-site VPN can enforce strict access controls, ensuring that only authorized users and devices can connect to the network. This reduces the risk of unauthorized access and helps protect sensitive government data.

7. Training and Preparedness: With a centralized network, it becomes easier to implement and manage cybersecurity training programs for employees. Regular training and simulations can enhance the preparedness of staff to recognize and respond to cybersecurity threats.

By integrating these features, a site-to-site VPN significantly strengthens the overall cybersecurity posture of state or local government systems, making them more resilient against potential risks and threats.

Does this explanation help? Feel free to ask if you have more questions!

7. 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.
A on-site contractor will collaborate with a remote engineer from the VPN vendor to configure a site-to-site VPN. This partnership ensures that the setup process is handled efficiently and effectively, leveraging the on-site contractor's presence and the remote engineer's specialized expertise. Together, they will work to establish a secure and reliable connection between the City Offices and the City Maintenance Department, enhancing the overall network infrastructure.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcomes of the site-to-site VPN project include:

1. Enhanced Security: Establish a secure, encrypted communication channel between the City Offices and the City Maintenance Department to protect sensitive data from unauthorized access and cyber threats.

2. Unified Network: Create a single, cohesive network that allows for seamless data sharing and collaboration between the two departments, improving overall operational efficiency.

3. Centralized Management: Enable centralized monitoring, auditing, and management of network traffic and security policies, ensuring consistent enforcement of security measures across all connected sites.

4. Improved Incident Response: Facilitate quicker detection and response to security incidents through centralized monitoring tools and real-time alerts, minimizing potential damage from cyber threats.

5. Increased Resilience: Enhance network resilience by providing redundant connections and robust disaster recovery capabilities, ensuring continuous operation and quick recovery in case of network failures or cyberattacks.

6. Compliance: Ensure adherence to regulatory requirements by providing detailed logs and reports of network activity, aiding in compliance audits and demonstrating adherence to security policies.

7. Web Filtering: Implement web filtering solutions to protect the City Maintenance Department from accessing malicious or inappropriate websites, thereby enhancing overall network security.

These outcomes aim to strengthen the cybersecurity posture, operational efficiency, and resilience of the city's network infrastructure.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☑ 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. 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.
This project is not scalable since it is a point to point solution.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89008

14. 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

15. 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

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab

- [ ] 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
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	**$ 0.00**	**$ 0.00**		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Firewall/Router	Firewall	1	$ 3,000.00	$ 3,000.00	1This is the main item for this project.	Currently, there is no funding to enhance security at this location. This location will continue as is with a home firewall device.	Firewall, Network	05NP-00-FWAL
Installation Cost		10	$ 180.00	$ 1,800.00	This will pay for the contractor to install the project.	After the installation, the city will pay for the contractor to maintain the system.		
			$	$				

			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
			$	$
		11	$ 3,180.00	$ 4,800.00

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		0	$ 0.00	$0.00			0

Document Uploads *top*

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

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

Application ID: 481860

	Applicant Name	City Of Caliente
	Project Name:	Site-toSite VPn
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Grant Writing and Approval	15-Oct
2	**Project Planning**:	15-Nov
3	**Vendor Selection**	1-Dec
4	**Network Assessment**	10-Dec
5	**Hardware and Software Procurement**	31-Dec
6	**Configuration and Setup**	15-Jan
7	**Training and Documentation**	20-Jan
8	**Implementation and Go-Live**	1-Feb
9	**Monitoring and Maintenance**	15-Feb
10	Project Review and Closure	1-Mar

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

City of Las Vegas

Southern Nevada Cyber Defense Project

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

$ 649,704.00 Requested

Submitted: 9/9/2024 4:51:22 PM (Pacific)

Project Contact
Carolyn Levering
clevering@lasvegasnevada.gov
Tel: 702220313

Additional Contacts
financegrantsteam@lasvegasnevada.gov

City of Las Vegas

495 S. Main Street
Las Vegas, NV 89101

Mayor
Carolyn G. Goodman
clevering@lasvegasnevada.gov

Telephone 7022290313
Fax
Web www.lasvegasnevada.gov
EIN 88-6000198
UEI HJS3TZHWWJX5
SAM Expires7/8/2020

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 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 Challenge: Currently, there is no way for government agencies to quickly share critical information when it comes to in-flight cyber-attacks. This causes us to always be a step behind when it comes to minimizing the business/operational risk because we are constantly living in a reactive state rather than a proactive state. We don't know another organization has been attacked until it has already happened, giving us little time to prepare/safeguard our organization.

Solution: The City of Las Vegas, Southern Nevada Health District, and University of Nevada, Las Vegas are partnering to create a Darktrace Unified Cloud Master View that will share and receive anonymized intelligence about unique threats discovered. No private data from the originating incident is shared, nor can the identity of the originating community member be reversed or discovered from the model breach. That said, any Southern Nevada government agency is open to join this initiative. Considering that City of Las Vegas is already leveraging Darktrace and its capabilities, Darktrace is the most suitable solution for our initiative. Moreover, the sole source document confirms that Darktrace is uniquely equipped to fulfill our requirements. Therefore, it appears that only Darktrace can effectively facilitate the connection to the Unified Cloud Master we aim to promote.

Outcome: By leveraging Darktrace's unique approach to cyber defense, we can help participating agencies proactively detect high-severity threats that have been identified elsewhere, and preemptively protect against threats that have not yet hit their systems and infrastructure.

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

Darktrace AI-driven approach to Cyber-Threat Detection autonomously monitors traffic detecting and investigating anomalous or suspicious behavior indicating potential cyber threats. This proactive approach allows for rapid containment of incidents and provides valuable insights for strengthening overall cybersecurity posture, ultimately reducing these participating government agencies exposure to cyber risks and cost.

Current State: Current systems lack automation and detection capabilities causing there to be a big reliance on slow, manual processes that waste critical time. There is no ability to learn behavior across the agencies and spot abnormal behavior proactively.

Future State: By creating a Darktrace Unified View, City of Las Vegas, Southern Nevada Health District, University of Nevada, Las Vegas and other participating agencies will leverage AI to identify subtle and emerging threats in real-time, as well as continually learn, adapt, and evolve to the changing environment. Darktrace increases visibility (14-minutes average to detect a threat vs industry average of 212 days), increases response time (seconds to respond to never-seen-before attacks, without disrupting normal business operations), reduces triage time (92% reduction in triage time), and improves efficiencies (5-10% reduction of actionable insights).

Business Outcomes: Save resources (AI automates investigation process saving 4-5 hours per analyst per week), save costs (cost of breach is avoided, cost of resources reduced, cost of solutions optimized with up to 40% reduction in security stack cost), reduce risk (risk of breach, reputational damage, potential GDPR fines, compliance violations and costly insurance premiums), and maintain continuity (incident closure rate improved by 20%).

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

Due to space limitations in this application, please refer to response to this question in the Document Uploads section.

7. 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.

The City of Las Vegas, Southern Nevada Health District, and University of Nevada, Las Vegas IT staff will work together along with any other participating government agencies on further enhancing their cyber security posture. Developing a Darktrace Unified View will provide all subsidiaries with the ability to stay ahead of fast-acting cyber-attacks by knowing at an early stage where potential threats are coming from and how they can best prepare.

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

The City of Las Vegas would like to create a threat intelligence ecosystem through the implementation of Darktrace's Cyber AI network solution. The idea would be that every government entity should have their own Darktrace deployment. Anonymized information can aggregate to the Unified View Cloud Master. Should any anomalous behavior or a breach occur, the anonymized information would be sent to the Unified View Cloud Master to give them early warning signs of a potential compromise. Ultimately, this should provide a symbiotic statewide intelligence ecosystem that provides threat sharing across all entities, while most importantly, protecting their network environment through Darktrace. Southern Nevada Health District and University of Nevada, Las Vegas will be part of Phase 1.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.

M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)

N/A

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?

EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.

- [ ] Yes
- [x] No

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).

- [x] Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- [ ] 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. 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, this project with Darktrace is scalable as it is industry and size agnostic. Darktrace can scale up or down seamlessly in accordance with the distribution of any digital environment. If a client would like to reduce visibility, it is as simple as reducing subnets to decrease the coverage. If a client wants to add additional locations, we can add additional appliances to the deployment scope. Scalability is one of Darktrace's differentiators and they are well-known in the industry for enabling a seamless journey for customers as they deploy and extend their platform.

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

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

89101, 89107 & 89154

14. 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.

- [x] Build
- [ ] Sustain

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

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.

Darktrace sits out-of-line from the core switch and passively ingests all raw network traffic via a SPAN session. This allows for continuous monitoring of the network traffic and activity. Darktrace's Self Learning AI will analyze the hundreds of thousands of connections to build a pattern of life for each unique asset, profile, peer group, and organization. By leveraging AI and unsupervised machine learning, Darktrace will be able to learn the normal behaviors within this environment and utilize mathematics to immediately spot anomalies and apply containment if necessary. Threats will be mapped to the MITRE attack framework, and each alert will also be mapped to the NIST framework. Darktrace will also alert the team to network risks such as the use of outdated protocols or unencrypted password files being transferred across the network to encourage best practices. All alerting in Darktrace can be configured to be sent externally to notify relevant stakeholders. Communication on alerting can also happen directly through the Darktrace UI by commenting on alerts and reports. Additionally, Darktrace can ingest threat intelligence for greater context and accuracy in detecting threats. Through a unified view, all agencies can anonymize information of threats and share threat intelligence by having a Cloud Master to host the shared threat intelligence.

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.

Leveraging advanced AI technology, Darktrace passively observes network traffic, analyzing patterns and behaviors to swiftly identify potential threats. Its continuous monitoring ensures comprehensive visibility into all activities, enabling timely detection of suspicious or unauthorized actions. Darktrace's sophisticated auditing capabilities offer detailed insights into network transactions, facilitating compliance with regulatory requirements, such as tracking user access to sensitive data to ensure adherence to standards like GDPR or HIPAA. In addition, Darktrace visibility can extend further than the network, reaching into SaaS, endpoint, SIEM, and other coverage areas through integrations, allowing for the monitoring of traffic across various platforms. Lastly, this solution does not only give visibility into this traffic, but gives actionable intel to security teams to understand what is going on in their environments. Administrators can utilize Darktrace to download packet captures, enabling detailed analysis of network traffic for forensic investigations. Darktrace can also provide comprehensive device summaries, offering insights into individual device status and behavior within the network. This level of granularity enables administrators to identify and address potential vulnerabilities, strengthening the overall network security posture. By providing these advanced capabilities, Darktrace equips state and local governments with the necessary tools to effectively monitor, manage, and secure their network infrastructure against evolving cyber threats.

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.

Through learning the everyday dynamics of your organization, Darktrace/Network can identify the subtle deviations from normal activity that indicate emerging threats – both known and unknown. It can then take proportionate action to neutralize an attack within seconds, minimizing business disruption. Darktrace DETECT + RESPOND products are designed to proactively detect, automatically investigate, and surgically respond to any type of threat. Darktrace RESPOND forms part of Darktrace's technology vision of a Cyber AI Loop, which empowers defenders to reduce cyber risk and disruption at every stage of the attack life cycle – from proactive measures taken to harden security before an attack gets in, to detecting and responding to an attack.

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.

Darktrace's continuous feedback loop consists of four AI engines that constantly feed back into the system, maintaining cyber stability for an organization. Darktrace/Network also combines Darktrace's attack surface management and attack path modeling capabilities to allow defenders to prioritize risk, while the AI hardens defenses around critical assets and attack paths.

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.

Darktrace's passive approach to cybersecurity aligns with ensuring continuity of communication and data networks within the jurisdiction of the state and between state and local governments. By "passive," Darktrace operates in real-time without disrupting normal network operations. It observes, learns, and detects anomalies or threats without requiring active intervention. This ensures that communication and data networks remain operational even during incidents, as Darktrace's continuous monitoring provides early detection and response to potential threats, thus minimizing downtime and ensuring the continuity of critical services. Crucially, Darktrace's response strategy is characterized by precision and proportionality, guaranteeing that our actions in response to threats are surgical rather than indiscriminate. For instance, rather than resorting to shutting down entire systems, Darktrace opts for measured and targeted actions to effectively mitigate specific threats which allows for business continuity. This approach preserves operational integrity while effectively addressing security concerns.

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.

By sharing intelligence across participating agencies, Darktrace can help mitigate risk and threats, by proactively alerting, detecting, and responding to threats.

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 Question 12 for further details on these services.)

Darktrace can create a unified view (UV) that receives data from all masters and their probes for display in a single user interface. Darktrace master instances under a UV operate as subordinate masters ("submasters"), where a subset of capabilities is removed and controlled/operated centrally at the UV level. Each master continues to operate a model engine and perform 'pattern of life analysis', but select components are synced downward from the UV (such as Darktrace models). Event data, such as that from modules and metadata produced by protocol analysis, is stored and analyzed on subordinate masters for retrieval by the UV. Darktrace provides a set of granular visibility restriction tools to ensure access is scoped to only the data each user should be permitted to see.

15. 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.

- [x] Yes
- [ ] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab

- [x] 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
- [x] Equipment - Equipment, supplies, and systems that comply with relevant standards
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Development of Unified View for Threat Intel	Quarterly meetings		0.00	$ 0.00	Quarterly meetings with Darktrace Team to discuss Unified View. This conversation will include the rollout of additional entities, recent findings, threat intel from Unified View, etc. It will be rolled out in Phases. This grant is for Phase 1	N/A
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	**$ 0.00**	**$ 0.00**		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
DETECT_RESPOND/Network	AI Powered Detection	1	$ 621,561.60	$ 621,561.60	AI Powered Detection covering 48,000 devices and Response covering 46,500 devices	One-time purchase	System, Intrusion Detecti	05NP-00-IDPS
Darktrace Deployment Usage Fees	Bundled usage fee	1	$ 28,142.40	$ 28,142.40	1 x Large (DCIP-XA) appliance, 2 x Large (DCIP-X2), 1 x Medium (DCIP-XA), Cloud	Recurring costs are shared by participating agencies	Hardware, Computer, Integ	04HW-01-INHW

					Master under 10k CPM will be needed for the deployment of UNLV and SNHD in Phase 1.
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
			$	$	
		2	$ 649,704.00	$ 649,704.00	

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
Services/Training/eLearning (Hosted)	Recorded video		$ 0.00	$ 0.00	Complimentary online training video modules via Darktrace Customer Portal	N/A	N/A
Services/Training/Public	Live online		$ 0.00	$ 0.00	Complimentary access to live online training sessions covering the full breadth of Darktrace's product suite and capabilities.	N/A	N/A
Services/Training/Private/Remote	Private remote		$ 0.00	$ 0.00	Darktrace will include 2 x free of charge personalized remote private trainings for City of Las Vegas	N/A	N/A
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
				$	$		
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	A-133 Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
		Payroll Narrative
Procurement Policy	☑	Procurement Policy
		Sole Source
Milestones download template	☑	Milestones
		2023 NCSR Certificate of Completion
		Budget Detail
		O6 Detailed Response

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

Application ID: 481389

Nevada Division of Emergency Management / Homeland Security

Prevent • Protect • Mitigate • Respond • Recover

Sole Source Request

Agency Name: City of Las Vegas

Email Address: clevering@lasvegasnevada.gov

Contact Name & Title: Carolyn Levering

Phone Number: (702) 229-0313

Project Name/FFY/Funding Source: State and Local Cybersecurity Grant Program FFY 2023

VENDOR/CONTRACT INFORMATION

Vendor Name: Darktrace

Contact Name: Aimee Levan

Complete Address: 6100 Center Drive Suite 1200, Los Angeles, CA 90045

Email Address: aimee.levan@darktrace.com

Phone: (323) 347-5587

Is the a **NEW CONTRACT**: YES ☑ NO ☐

Contract Start Date: TBD

Contract End Date: TBD

Estimated Value of this Contract: $649,704.00

Clearly and succinctly describe the Work/Services/Purchase:

Leveraging advanced AI technology, Darktrace passively observes network traffic, analyzing patterns and behaviors to swiftly identify potential threats. Its continuous monitoring ensures comprehensive visibility into all activities, enabling timely detection of suspicious or unauthorized actions. Darktrace's sophisticated auditing capabilities offer detailed insights into network transactions, facilitating compliance with regulatory requirements, such as tracking user access to sensitive data to ensure adherence to standards like GDPR or HIPAA. In addition, Darktrace visibility can extend further than the network, reaching into SaaS, endpoint, SIEM, and other coverage areas through integrations, allowing for the monitoring of traffic across various

Per SAM 0326(8), a Sole Source Waiver is ***not*** required for computer software maintenance that consists of the following: license agreements, right to download updates remotely and/or off-site technical support. This does not exempt an agency from following any other processes that may be required (i.e., entries into *NevadaEPro*, agency specific approvals or authorizations, etc.).

Discribe the unique features or qualifications required of this vendor that are not available through other vendors:
Please refer to 2 CFR 200.320 Part C and NRS 333.300 for complete description

Per SAM 0326(8), a Sole Source Waiver is not required for computer software maintenance that consists of the following: license agreements, right to download updates remotely and/or off-site technical support.

Per 2 CFR 200.320 Part c, noncompetitive procurement can be awarded if:
-- The item is available only from a single source;
-- The Federal awarding agency or pass-through entity expressly authorizes a noncompetitive procurement in response to a written request from the non-Federal entity;
-- After solicitation of a number of sources, competition is determined inadequate.

Sole Source Request

Were alternative Work/Services/Purchases evaluated? YES ☐ NO ☑

If **YES** why were they not acceptable/If **NO** why were alternatives not evaluated and please be specific:

Per NRS 332.115.1(h), software for computers is eligible for competitive bidding exception. The original 2016 contract with Darktrace was awarded under a competitive bidding exception with the following justification:
Darktrace is a sophisticated, proprietary and highly innovative security monitoring system that allows the Information Technologies Department to monitor for advanced persistent threats (APTs) to internal computer and communications systems. This advanced system provides an elevated level of protection to our critical infrastructure, which currently does not exist.

Through the use of an evolving behavioral analysis algorithm and by identification of

Is this a **1 TIME PURCHASE**: YES ☐ NO ☑

If this request is for an ongoing project, describe in detail all dates and work/equipment to be completed:

Contract Execution 7/30/2024
Kick Off & Deployment Rollout Discussion 8/1/2024
Provide UI & Customer Portal Access to Team 8/1/2024
Tuning & Tagging Session for Respond Capabilities (Phase 1: Passive Mode) 8/9/2024
Private Remote Training 8/15/2024
Tuning & Tagging Session for Respond Capabilities (Phase 2: Human Confirmation Mode) 8/22/2024
Unified View Successfully Sharing Threat Intel (Go Live) 9/19/2024
Tuning & Tagging Session for Respond Capabilities (Phase 3: Autonomous Mode) 9/26/2024
Contract Expiration Review Begins 10/18/2024

If this vendor has been used before, starting with the most recent contract, list the entire relationship:

Short Discription	Value	Term	
		Start Date	End Date
Darktrace license agreement for security software	$160,800	6/23/2016	8/1/2020
Darktrace license expansion	$423,261.77	3/22/2018	6/30/2022
Addition of Darktrace DETECT system for threat monitoring and response	$107,000	3/29/2023	6/30/2025

By Signing below, I understand that this agreement will be terminated should any of the information provided be found untrue.

City of Las Vegas, NV

Name of Agency Requesting a Sole Source Purchase

Carolyn Levering

Print Name of Authorized Agency Representative Initiating Request

6/26/2024

Signature of Authorized Agency Representative / Electric Signatures are Accepted — Date

This Sole Source Request must be submitted by email with all pertinent backup documentation
Email Address for DHSGrants: DHSGrants@dem.nv.gov

Sole Source Request

Additional Information:

For searching of State Contracts:
https://nevadaepro.com/bso/view/search/external/advancedSearchContractBlanket.xhtml?view=activeContracts

For Governmental Entities only: If you wish to use NevadaEPro for placing of orders with contracted vendors, please have your purchasing department contact Gideon Davis at gkdavis@admin.nv.gov

For DEM Use Only

After reviewing all of the information contained in this Sole Source Request, I ____ Approve / ____ Deny this Sole Source Request

Comments of Reviewer:

Print Name and Title of Authorized Agency Representative Reviewing this Reques

Signature of Autorized Agency Representative Date

	Applicant Name	City of Las Vegas
	Project Name:	Dartrace - Unified View for Threat Intel
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Contract Execution	7/30/2024
2	Kick Off & Deployment Rollout Discussion	8/1/2024
3	Provide UI & Customer Portal Access to Team	8/1/2024
4	Tuning & Tagging Session for Respond Capabilities (Phase 1: Passive Mode)	8/9/2024
5	Private Remote Training	8/15/2024
6	Tuning & Tagging Session for Respond Capabilities (Phase 2: Human Confirmation Mode)	8/22/2024
7	Unified View Successfully Sharing Threat Intel (Go Live)	9/19/2024
8	Tuning & Tagging Session for Respond Capabilities (Phase 3: Autonomous Mode)	9/26/2024
9	Quarterly Executive Business Review	10/12/2024
10	Continued Conversations with Other Agencies Interested in Joining Unified View	11/7/2024
11	Begin Phase 2 of Unified View	11/14/2024
12	Phase 1 of Unified View Completed	12/6/2024

* These are the originally proposed milestone dates.

Based on date of award execution, milestone 1 will be completed within 6 months; remaining milestones to follow in succession.

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

City of Reno

Cloud Backup & On Premise Backup Assessment

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

$ 299,736.00 Requested

Submitted: 9/27/2024 3:37:43 PM (Pacific)

Project Contact
Mark Stone
stonema@reno.gov
Tel: 7753343105

Additional Contacts
Phelpsa@reno.gov,hancockb@reno.gov

City of Reno

PO Box 1900
Reno, NV 89505
United States

Director of Finance
Vicki Van Buren
vanburenv@reno.gov

Telephone	775-334-3105
Fax	
Web	reno.gov
EIN	88-6000201
UEI	TH74SE96JVC7
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 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 City of Reno is seeking to assess our backup strategy and remediate any security holes.

We currently own a backup and recovery system for on premise servers, along with an additional security appliance. We believe the configuration of the current backup solution is not immutable and may be at risk in the event of a cyber attack. Items such as multiple admin codes to make changes, encrypted backups, air gapped management interface, data replication to failover site, and other items require configuration. We need an assessment and configuration assistance to ensure we are getting the best resilience out of our existing on prem backup appliance.

The backup system also includes a security clean room appliance to validate a backup is free of malware before restoring is sitting unconfigured without the appropriate knowledge to configure it.

In addition to strengthening our on premise environment we have no backup solution for our cloud environment, we currently only have the ability to restore from the native retention tools and aren't considered to be comprehensive disaster recovery backups. This grant would allow us to implement a new backup solution for this environment that doesn't exist currently.

5. How does your project align with the objective selected in Question 2?
The City of Reno's current backup solution is sufficient for restoring individual files/directories that are deleted or a technical issue with an on premise server, but the configuration of the appliance as it stands now is not air gapped and missing critical security controls and features. Without these protections in place the ability for an attacker to wipe out both the backups and production systems in a wiper/ransomware scenario are far greater and may be forced into paying a ransomware if backups don't survive.

The same scenario can apply to our cloud tenant in the event an attacker gained elevated privileges to delete the data and configurations in the cloud with default retention functions.

This project allows us to be more resilient in the event of a cybersecurity attack and able to restore quicker than the alternative scenario of no backups to recover from. It also improves the ability to ensure continuity of critical City operations such as Public Safety Dispatching for all Washoe County Citizens, Waste Water Treatment Facilities, and other critical infrastructure.

6. How does your project align with the program element(s) selected in Question 3?
By implementing these 3 projects we are enhancing our preparation to any sort of attack by ensuring data is recoverable in an attack, which greatly increases our ability to respond and recover in the event an attacker is successful. It also brings our backup solutions into line with industry best practices and with the knowledge other governments and incidents responders are seeing in attacks that the backups are usually the first target to cripple before launching their main ransomware attack. Reno currently maintains the regional 911 CAD system for all of Washoe County emergency services as well as Waste Water Treatment so ensuring quick recovery so communication for critical infrastructure between Reno, Washoe, Sparks, UNR, RSIC, PLPT, Reno Airport, and TMWA is paramount.

7. 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.
Our Senior Cybersecurity Analyst along with our Senior Network Analyst and Network Analyst will work directly with the vender consultant/engineers to perform the assessment and apply any recommended reconfigurations as well as bring the undeployed cyber recovery appliance online. Reno staff will also stand up the cloud backup solution, security hardening, and data repository per vender best practices guides and the Senior Cybersecurity Analyst acting as the auditing oversight. Staff will dedicate their time to ensure all elements of this strategy are implemented to completion.

8. Describe, in a few sentences, the desired outcome(s) of your project.
Backup solutions and security settings will be shored up or implemented that don't exist at all currently to greatly increase the likelihood of being able to survive an attack or critical hardware/cloud failure. By the end of the project backup immutability, multiple admin codes required for overrides, backup MFA, and air gapping of the backup appliance will be implemented to the fullest extent possible. Cloud backups that don't exist at all currently will be implemented and follow the same security best practices as the On Prem appliance where ever possible.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
Understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.

- [ ] Yes
- [x] No

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).

- [x] Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- [ ] 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. 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.
There are three parts to our backup security enhancements. You can approve one, two or all three. They are not dependent on one another but each one compliments our strategy.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89501

14. 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.

- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab

- [x] 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
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Cyber Recovery Appliance Configuration	Configuration assistance of a security appliance.	1	30,000.00	$ 30,000.00	This project will enhance our backup strategy which admittedly has some lacking security features configured. This cyber recovery appliance is sitting unconfigured and unused. We need assistance in configuring it to industry standard while utilizing all security features. Currently if we restored from backup there is no way to validate the data is free from infection before returning it to the prod environment.	This is a one time need.
Backup Solution Security Assessment	Security assessment/review of our current on premise backup solution.	1	70,000.00	$ 70,000.00	Our current backup solution hassecurity weaknesses and lacks critical hardening best practices along with unused security features. An assessment will give us a clear picture of those security gaps and allow the vendor and our staff to work on remediation of those issues.	This is a one time need.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		2	**100,000.00**	**$ 100,000.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
			0	**$ 0.00**	$ 0.00			

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Cloud Backup Solution	Backup solution for our cloud environment.	1	$ 169,736.00	$ 169,736.00	Our main cloud environment is not currently backed up. If an attacker gained access we do not have a way to recover potential data lass and native tools Microsoft tools do not protect this scenario. This would enhance our backup strategy as a whole and fill in a large missing element.	Funding will be requested through our annual budget process.	Applications, SAAS	04AP-11-SAAS
Cloud Backup Storage	Storage needed for the cloud backup solution.	1	$ 30,000.00	$ 30,000.00	Cloud Storage bucket required for holding backup files that are generated by the backup application.	Funding will be requested through our annual budget process.	Applications, SAAS	04AP-11-SAAS
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
				$ $				
		2	**$ 199,736.00**	$ 199,736.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			

			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

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 Purchasing Policy
Milestones download template	☑	Grant Milestones
		Capabilities Assessment

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

Application ID: 481533

	Applicant Name	City of Reno
	Project Name:	Cloud Backup & On Premise Backup Assessment
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Project RFP	1/1/2025
2	On Premise Assessment Implementation	3/1/2025
3	Cloud Backup Implementation	3/1/2025
4	Security Appliance Configuration	3/1/2025
5	On Premise Assessment Review	4/1/2025
6	Cloud Backup Completion	4/15/2025
7	Security Appliance Complete	3/15/2025
8	On Premise Configuration Changes	4/7/2025
9	On Premise Complete	5/1/2025
10		

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Douglas County
Cloud Data Backup

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

$ 82,500.00 Requested

Submitted: 9/26/2024 3:42:05 PM (Pacific)

Project Contact
Debbie Swickard
dswickard@douglasnv.us
Tel: 775-782-9029

Additional Contacts
pruggia@douglasnv.us,keaston@douglasnv.us,evelina.Burnett@iparametrics.com

Douglas County

1594 Esmeralda Ave
Minden, NV 89423-0218
United States

Chief Financial Officer
Kathy Lewis
klewis@douglasnv.us

Telephone	0
Fax	0
Web	https://www.douglascountynv.gov/
EIN	88-6000031
UEI	KE5GF37F6F95
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 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.

- [x] 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.
- [x] 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 Question 12 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?
Evaluating and implementing cloud backups for a Microsoft 365 tenant, involves several steps to ensure data security, reliability, and compliance. Target the following areas: exchange, sharepoint, onedrive and teams.

Search for a backup solution that will be compliant with CJIS, HIPAA. This provides improvement and remediation paths for data that resides in Microsoft 365.

5. How does your project align with the objective selected in Question 2?
Provides industry standard backups and immutable logs. Provides data security and business continuity in case of cybersecurity attacks, account compromises or data corruption. Reliance on Microsoft 365 data is high and mission critical to continuity of service for all of our departments and County services. There's definite risk on relying on Microsoft to safeguard data. There's no remediation or recovery when the account data is compromised and modified.

6. How does your project align with the program element(s) selected in Question 3?
Ensures the continuity of communication and data networks within the state's jurisdiction, facilitating reliable interaction between state and local governments during incidents that impact these networks. Protection against malware, ransomware, internal threats and attacks, and solves regulatory compliance requirements.

7. 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.
Internal staff members will evaluate and pick software based on a search criteria that consists of: core functionality, usability, scalability, security, support and maintenance and training. Once the decision is made on the backup solution, internal staff will work with the vendor to implement the solution.

8. Describe, in a few sentences, the desired outcome(s) of your project.
Will have cloud to cloud backups for our Microsoft 365 tenant. There will be an ability to backup all users, emails, files, chats. And an ability to recover in the event of a cybersecurity attack. Additionally, have immutable logs which will safeguard the County from internal attack and unauthorized access.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
I understand.

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.

- [ ] Yes
- [x] No

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), either on our own or as a condition of FY 2022 SLCGP
- [x] 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. 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.
The project is scalable because we would be able to find a solution that could scale up to include cloud backups for servers. This would be a logical next step in our backup solution maturity.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89423

14. 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.
- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [ ] 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
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	0.00	$ 0.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		

EQUIPMENT COSTS

					Describe how the purchase(s)	How would

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Cloud backup solution	Divided up by protection per user.	550	$ 150.00	$ 82,500.00	The tenant backup cloud to cloud would be utilized per user to protect the user from data loss. And safeguard against cybersecurity threats	Hopefully, I can show value in the backup safeguarding of the data and find funding permanently. Otherwise, we would look for other grant funding.	SAAS	04AP-11
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		550	**$ 150.00**	**$ 82,500.00**				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	**$ 0.00**			**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	**$ 0.00**			**0**

Total	0	$ 0.00 $0.00	0

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	2023 SEFA Audit
Travel Policy	☑	300.06 Travel Policy
Payroll Policy	☑	200.11-46 Payroll Policies
Procurement Policy	☑	300.19 Procurement Policy & Procurement Fact Sheet
Milestones download template	☑	Douglas County Cloud Data Backup - Milestones

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

Application ID: 482996

Outlook

Re: OCDC - State and Local Cybersecurity Grant Program 2023 Application for Leftover Funds

From Evelina Burnett <Evelina.Burnett@iparametrics.com>
Date Fri 09/27/24 10:17 AM
To Amanda Jackson <amanda.jackson@dem.nv.gov>
Cc Swickard, Debbie <DSwickard@douglasnv.us>; Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Peace Ruggia <pruggia@douglasnv.us>

Good morning, Amanda - I just spoke with Peace, and he explained that the 2022 request was for hardware/equipment for our data center. The current request is for software that would allow a cloud-to-cloud backup of our Microsoft Office 365 data.

Please let us know if you need more details or if you have any other questions!
Evelina

From: Amanda Jackson <amanda.jackson@dem.nv.gov>
Sent: Friday, September 27, 2024 10:59 AM
To: Evelina Burnett <Evelina.Burnett@iparametrics.com>
Cc: Swickard, Debbie <DSwickard@douglasnv.us>; Anjelicah Y. Garcia <a.garcia@dem.nv.gov>; DHSGrants <DHSGrants@dem.nv.gov>; Peace Ruggia <pruggia@douglasnv.us>
Subject: Re: OCDC - State and Local Cybersecurity Grant Program 2023 Application for Leftover Funds

Good morning,

I appreciate you all getting an application in! I just started reviewing it and I have one question to start: How is the 2024 project different from the 2022 Backup Datacenter Environment project for which Douglas County was awarded? Bear in mind, I am not a cybersecurity person, so to the trained eye they might be completely different, I'm just not seeing it so I need some help! I've attached both applications for convenience.

Thank you!

Amanda Jackson
Grants & Projects Analyst II, Southern Nevada
Office Hours: Mon-Fri, 7:00am-4:00pm

	Applicant Name	Douglas County
	Project Name:	Cloud Data Backup
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Project Initiation	11/1/2024
2	Requirements Gathering	11/30/2024
3	Vendor Search and Shortlist	12/31/2024
4	Vendor Demo and Evaluation	3/1/2025
5	Decision and Selection of Vendor	3/30/2025
6	Contract Negotiation	4/30/2025
7	Implementation Plan	5/15/2025
8	Configured and Deployment	6/30/2025
9		
10		

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Las Vegas Paiute Tribe

Las Vegas Paiute Tribe Cyber Posture Upgrade

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

$ 74,800.00 Requested

Submitted: 9/25/2024 10:04:26 AM (Pacific)

Project Contact
Estevan Roman
eroman@lvpaiute.com
Tel: 702-383-1520

Additional Contacts
none entered

Las Vegas Paiute Tribe

1 Paiute Dr
Las Vegas, NV 89106
United States

Controller
Brent Hilton
bhilton@lvpaiute.com

Telephone	702-383-1520
Fax	
Web	https://www.lvpaiutetribe.com/
EIN	88-0135111
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 12. Leverage cybersecurity services offered by CISA. (See Question 12 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?
Would like to replace servers, workstations and firewalls with newer versions that are up to date with security standards and supported by the vendors. With the vendors no longer supporting the devices, we cannot update the operating systems with security patches such as Zero-Day exploits or other found vulnerabilities thus leaving the Tribe much more vulnerable to hacking. This is especially important for our Law Enforcement department.
We also need to implement backup solutions for our locations, particularly our Law Enforcement who do not have backups at this time due to budget constraints.

5. How does your project align with the objective selected in Question 2?
It would increase our cybersecurity posture, improve our response to any incidents decrease the chance of an attack which would help us to ensure a better continuity of operations.

6. How does your project align with the program element(s) selected in Question 3?
All the areas checked off such as assessing and mitigating would be much simpler to accomplish as our current licensing and software does not allow for this, we can also implement NIST recommended best practices.

7. 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.
Servers, workstations will be replaced and configured to the NIST/CISA standards for security settings using CISA recommended tools for configuring said settings.
Firewall which are currently unsupported and not licensed for increase security standards would be configured with recommended settings such as IPS/IDS, DPI and alert notifications.
This work will be performed by the internal IT department under the guide of the IT Director.

8. Describe, in a few sentences, the desired outcome(s) of your project.
To increase our cybersecurity resiliency and lower the risk of the Tribe coming under a cybersecurity attack and if one does come, also decrease the risk of downtime to our operations as well as mitigate any losses occurred.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
Understand.

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.

- [ ] Yes
- [x] No

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).

- [x] Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- [ ] 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. 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, certain items of the projected purchases such as the firewall and computer equipment can be scaled to have more or less memory, hard drive space and the firewalls can be scaled up to include EDR capabilities.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89106

14. 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.

- [x] Build
- [ ] Sustain

15. 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
- [x] No

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

Each selection should have an accompanying item in the line item detail budget table on the next tab

- [ ] 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
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	0.00	$ 0.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Workstation	New Workstation	3	$ 700.00	$ 2,100.00	Computer hardware and operating system software designated for use in an integrated	Would rely on obtaining capital expenditures if budgetary sources can be found.	Hardware, Computer, Integ	04HW-01-INHW

					system allowable under the indicated grant programs. Such systems include detection, communication, cybersecurity, logistical support and Geospatial Information Systems. This item may include networking hardware (routers, wireless access points, etc. servers, workstations, notebook computers, and peripherals such as printers and plotters procured with an allowable system and necessary for its implementation.				
Monitors	Monitors	6	$ 160.00	$ 960.00	Computer hardware and operating system software designated for use in an integrated system allowable under the indicated grant programs. Such systems include detection, communication, cybersecurity, logistical support and Geospatial Information Systems. This item may include networking hardware (routers, wireless access points, etc. servers, workstations, notebook computers, and peripherals such as printers and plotters procured with an allowable system and necessary for its implementation.	Would rely on obtaining capital expenditures if budgetary sources can be found.	Hardware, Computer, Integ		04HW-01-INHW
Servers	New Servers	3	$ 8,500.00	$ 25,500.00	Computer hardware and operating system software designated for use in an integrated system allowable under the indicated grant programs. Such systems include detection, communication, cybersecurity, logistical support and Geospatial Information	Would rely on obtaining capital expenditures if budgetary sources can be found.	Hardware, Computer, Integ		04HW-01-INHW

					Systems. This item may include networking hardware (routers, wireless access points, etc. servers, workstations, notebook computers, and peripherals such as printers and plotters procured with an allowable system and necessary for its implementation.			
Firewall	Firewall Replacement	5	$ 6,600.00	$ 33,000.00	Firewall (software or standalone appliance) for use in protecting networks.	Would rely on obtaining capital expenditures if budgetary sources can be found.	Firewall, Network	05NP-00-FWAL
Network Attached Storage	NAS Device	2	$ 1,500.00	$ 3,000.00	NAS device for providing backup storage if in the event we are hit with a security event.	Would rely on obtaining capital expenditures if budgetary sources can be found.	Hardware, Computer, Integ	04HW-01-INHW
Backup Software	Veeam Backup Software	1	$ 2,140.00	$ 2,140.00	Software or systems that facilitate capture, quantification, and management of risk factors involved in specific tasks, environments, or programs. This functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software. However, special security considerations apply for data stored remotely.	Would rely on obtaining capital expenditures if budgetary sources can be found.	oftware, Risk Management	04AP-04-RISK
Laptops	Laptops	3	$ 1,500.00	$ 4,500.00	Mobile computer devices, usually mounted permanently in vehicle, operating from DC power supply. Used for data upload and download, as well as local data entry.	Would rely on obtaining capital expenditures if budgetary sources can be found.	Computer, Mobile Data	04HW-01-MOBL
Window Server Licensing	Operating System Software	3	$ 1,200.00	$ 3,600.00	Latest operating system software that would ensure the server is using the most up to date and secure version of the server software that is supported and able to patch any security flaws.	Would rely on obtaining capital expenditures if budgetary sources can be found.	Hardware, Computer, Integ	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				

		$	$	
	26	$	$	
	22,300.00	74,800.00		

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

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

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

Application ID: 482208

	Applicant Name	Las Vegas Paiute Tribe
	Project Name:	Las Vegas Paiute Tribe Cyber Posture Upgrade
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Install workstations and displays	12/31/2024
2	Replace Servers	2/28/2025
3	Install new firewall	2/28/2024
4	Setup NAS Devices	2/28/2025
5	Install and configure backup software	2/28/2025
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

LVMPD

LVMPD Cyber Security Project FFY23

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

$ 404,042.00 Requested

Submitted: 9/13/2024 2:27:11 PM (Pacific)

Project Contact
Diana Clarkson
d14977c@lvmpd.com
Tel: 702-828-2257

Additional Contacts
none entered

LVMPD

400 S Martin Luther King Blvd
Las Vegas, NV 89106
United States

Sheriff
Kevin McMahill
j13700p@lvmpd.com

Telephone	702-828-2831
Fax	
Web	
EIN	0000000000
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 for further details on these services.)
- [x] 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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?
This project will sustain current capabilities funded by UASI, this project directly aligns with the strategic priority of enhancing cybersecurity. The threat of a cyber-attack against local government agencies has increased dramatically. The purpose of this proposed project is to better target harden the largest law enforcement agency in the state of Nevada by increasing our security posture to counter terrorism threats by utilizing established industry best practices. This will involve two security support analysts, cybersecurity training, ransomware protection with KnownBe4 or something similar, and privilege access for risk management through Thycotic Privilege or a program similar. A major cyber incident at the LVMPD would not only impact our agency, it would impact over 40 federal/state/county/city partner agencies within the state of Nevada. These IT resources play an integral role in sharing public safety information among partner agencies as well as protecting the community. The project's goal is to ensure that Law Enforcement is able to adequately prevent, detect, deter and respond to acts of terrorism. Without appropriate cybersecurity protecting our systems, law enforcement would be severely disrupted.

5. How does your project align with the objective selected in Question 2?
Implement security protections commensurate with risk. This will involve full-time dedicated cyber security professionals that will enhance the security of the LVMPD network and assist the with following industry best practices in regard to cyber security and target hardening. KnownBe4 is the world's largest and most comprehensive integrated Security Awareness Training and Simulated Phishing platform with tens of thousands of active enterprise accounts. This provides a highly effective platform to better manage the urgent IT security problems of social engineering, spear-phishing, and ransomware attacks and at the same time stay compliant with industry regulations like PCI, HIPAA, SOX, FFIEC and GLBA.The KnowBe4 platform allows the LVMPD to provide mandatory cyber security awareness training on a continued basis to employees, which dramatically increases the security posture of the LVMPD. Thycotic Behavioral Analytics provides a cloud-based solution that utilizes advanced machine learning technology to analyze privileged account activity within Thycotic Secret Server and alert for anomalous or suspicious user behaviors. The issue is 62 percent of cyber security breaches from hackers or abuse by malicious insiders involve compromised privileged account credentials. These attacks are hard to discover and can go undetected for months. Examples of capabilities include two factor authentication, role-based access control, web password filler, password hiding, IP restrictions, and various service management capabilities.

6. How does your project align with the program element(s) selected in Question 3?
Our project aligns with multiple elements. The Las Vegas Metropolitan Police Department (LVMPD) is the largest law enforcement agency in the state of Nevada. The LVMPD jurisdiction encompasses all of Clark County, Nevada. Within Clark County, there are multiple law enforcement agencies and government partners who utilize and rely upon LVMPD managed information technology (IT) resources. These IT resources play an integral role in sharing public safety information among partner agencies as well as protecting the community. Without appropriate cybersecurity protecting our systems, law enforcement would be severely disrupted. The project's goal is to ensure that Law Enforcement is able to adequately prevent, detect, deter and respond to acts of terrorism. Without appropriate cybersecurity protecting our systems, law enforcement would be severely disrupted.

7. 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.
This project will be administered by LVMPD's Business and Technology and Support Division as well as LVMPDs Cyber Security Incident Response Team Committee (CSIRTC). LVMPD will map out this phased response for enhancing cyber security, and better target harden an already ideal target to threat actors.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The threat of a cyber-attack against local government agencies has increased dramatically. The goal of this proposed project is to better target harden the largest Law Enforcement agency in the state of Nevada, LVMPD, by increasing our security posture to counter terrorism threats by utilizing established industry best practices. This will involve cybersecurity training, ransomware protection, and privilege access for risk management. A major cyber incident at the LVMPD would not only impact our agency, it would impact over 40 federal/state/county/city partner agencies within the state of Nevada. The LVMPD Cyber Security Incident Response Team (CSIRT) committee has made several recommendations that will enhance the security of the LVMPD network and assist the LVMPD with following industry best practices with regard to cyber security and target hardening.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
N/A

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- [ ] Yes
- [x] No

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).
- [x] Our agency is already participating in the Cyber Hygiene Services and Nationwide Cybersecurity Review (NCSR), either on our own or as a condition of FY 2022 SLCGP
- [ ] 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. 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.
No, to reduce this grant would pull capability away.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89106

14. 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

15. 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

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- ☐ 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
(2) Security Support Analyst Positions	(2) Security Support Analyst Positions	2	$ 131,021.00	$ 262,042.00	Implement security protections commensurate with risk. This will involve full-time dedicated cyber security professionals that will enhance the security of the LVMPD network and assist the with following industry best practices in regard to cyber security and target hardening.	Positions would be funded by the organization.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		2	**$ 131,021.00**	**$ 262,042.00**		

EQUIPMENT COSTS

Describe how

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
KnownBe4 Security Awareness Training	KnownBe4 Security Awareness Training	1	$ 58,500.00	$ 58,500.00	KnownBe4 is the world's largest and most comprehensive integrated Security Awareness Training and Simulated Phishing platform with tens of thousands of active enterprise accounts. This program or something similar provides a highly effective platform to better manage the urgent IT security problems of social engineering, spear-phishing, and ransomware attacks and at the same time stay compliant with industry regulations like PCI, HIPAA, SOX, FFIEC and GLBA.	We would lose this capability	Software, Malware/Anti-Vi	05HS-00-MALW
KnownBe4 PhishER Subscription	KnownBe4 PhishER Subscription	1	$ 25,500.00	$ 25,500.00	The KnowBe4 platform or something similar allows the LVMPD to provide mandatory cyber security awareness training on a continued basis to employees, which dramatically increases the security posture of the LVMPD.	We would lose this capability	Software, Network	04SW-04-NETW
Thycotic Privilege Access Management	Thycotic Privilege Access Management	1	$ 58,000.00	$ 58,000.00	Thycotic Behavioral Analytics or something similar provides a cloud-based solution that utilizes advanced machine learning technology to analyze privileged account activity within Thycotic Secret Server and alert for anomalous or suspicious user behaviors.	We would lose this capability	Software, Malware/Anti-Vi	05HS-00-MALW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				

			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		3	$ 142,000.00	$ 142,000.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	Single audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Grant Milestones

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

Application ID: 481433

Applicant Name	Diana Clarkson	
Project Name:	LVMPD Cyber Program - FY23	
Project Funding Stream:	FY 2023 SLCGP	
Milestone Name	Date Expected Complete	
Personnel costs	Ongoing personnel costs, payroll bi-weekly	1
KnownBe4 Training	Ongoing services, billed monthly	2
KnownBe4 Subscription	Ongoing services, billed monthly	3
Thycotic Privilege Access Management	Ongoing services, billed monthly	4
		5
		6
		7
		8
		9
		10

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Nevada Department of Agriculture

NDA Cyber Security Risk Gap Assessment

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

$ 25,500.00 Requested

Submitted: 9/27/2024 2:39:50 PM (Pacific)

Project Contact
Jake Dawley
j.dawley@agri.nv.gov
Tel: 7753533645

Additional Contacts
cbalcon@agri.nv.gov

Nevada Department of Agriculture

405 S 21st St
Sparks, NV 89431
United States

Administrator, Administrative Services Division
Cathy Balcon
cbalcon@agri.nv.gov

Telephone	7753533601
Fax	
Web	
EIN	88-6000002
UEI	TUFEHHFJ2P79
SAM Expires	2/26/2025

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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 Question 12 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?

Project Goal: To strengthen the Nevada Department of Agriculture's (NDA) cybersecurity resilience by conducting a comprehensive gap assessment against the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Key Objectives:

- Identify and address critical security gaps.
- Prioritize mitigation strategies based on risk.
- Enhance data protection and reduce cyberattack risks.
- Align with industry best practices and regulatory requirements.
- Foster a culture of cybersecurity within NDA.

Rationale:

By aligning with the NIST CSF, NDA can establish a standardized framework for assessing and improving its cybersecurity posture, ensuring the protection of sensitive data and continuity of operations.

Project Benefits:

- Improved cybersecurity posture
- Enhanced data protection
- Reduced risk of cyberattacks
- Compliance with industry standards
- Continuous improvement

This project aligns directly with the goals of the state & local government cybersecurity grant program by providing a comprehensive approach to enhancing NDA's cybersecurity capabilities and protecting critical infrastructure.

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

This project aligns directly with Objective 2 of the state & local government cybersecurity grant program. The NIST CSF gap assessment will provide NDA with a comprehensive understanding of its current cybersecurity posture by:

- Identifying gaps and vulnerabilities: The assessment will pinpoint weaknesses in NDA's existing security controls, providing a clear picture of areas requiring improvement.
- Prioritizing risks: By identifying critical vulnerabilities, NDA can focus its resources on addressing the most significant threats to its operations.
- Establishing a baseline: The assessment will serve as a baseline for ongoing cybersecurity efforts, enabling NDA to track progress and identify areas for continuous improvement.

Key Activities:

- Conducting a comprehensive gap assessment: The project will involve a detailed evaluation of NDA's security controls against NIST CSF best practices.
- Identifying critical vulnerabilities: The assessment will prioritize vulnerabilities based on their potential impact on NDA's operations.
- Developing a remediation plan: Based on the assessment findings, NDA will develop a targeted plan to address identified gaps and vulnerabilities.

This project is a crucial step in achieving Objective 2 by providing NDA with a clear and actionable understanding of its current cybersecurity posture and areas for improvement. By addressing these vulnerabilities, NDA can significantly enhance its resilience and protect critical infrastructure.

6. How does your project align with the program element(s) selected in Question 3?
Program Element 3: Enhance the preparation, response, and resilience of information systems, applications, and user accounts...

Direct Alignment: This project aligns strongly with Program Element 3. By identifying and addressing security gaps, NDA will enhance the resilience of its information systems and user accounts against cybersecurity threats.

Improved Preparedness: The project will enable NDA to develop a more effective response plan by providing a clear understanding of potential risks and vulnerabilities.

Program Element 4: Implement a process of continuous cybersecurity vulnerability assessments...

Direct Alignment: This project is a foundational step in implementing a continuous vulnerability assessment process. The NIST CSF gap assessment will provide a baseline for ongoing monitoring and evaluation.

Prioritized Mitigation: By identifying and prioritizing risks, NDA can focus its resources on addressing the most critical threats, ensuring that mitigation efforts are aligned with the highest priorities.

Program Element 5: Ensure that the state or local governments... adopt and use best practices...

Direct Alignment: The NIST CSF is a widely recognized cybersecurity framework that embodies best practices. By aligning with the NIST CSF, NDA is demonstrating its commitment to adopting and using best practices in cybersecurity.

Improved Security Posture: Adhering to NIST CSF standards will help NDA strengthen its security posture and reduce the risk of cyberattacks.

Conclusion:

This project aligns strongly with all three program elements. By conducting a NIST CSF gap assessment, NDA will enhance its cybersecurity preparedness, implement a process of continuous vulnerability assessment, and adopt best practices to improve its overall security posture.

7. 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.
A third-party vendor will be selected through the state's procurement process to conduct the assessment. The vendor will work closely with NDA staff to identify security gaps, prioritize risks, and develop targeted remediation strategies. This project will provide NDA with a clear understanding of its current security posture and enable it to implement necessary measures to protect its critical infrastructure and data.

Vendor Selection:

- Identify Qualified Vendors: Research and identify potential vendors with expertise in NIST CSF assessments and a track record of successful projects.
- Request Proposals: Invite selected vendors to submit proposals outlining their approach, methodology, and pricing.
- Evaluation and Selection: Evaluate proposals based on factors such as experience, expertise, references, and alignment with project goals.
- Contract Negotiation: Negotiate terms and conditions of the vendor contract, ensuring alignment with NDA's requirements and budget.

Vendor Coordination and Support:

- Project Kickoff: Conduct a project kickoff meeting to establish clear expectations, timelines, and communication channels.
- Data Provision: Provide necessary data and access to systems for the vendor to conduct the assessment.
- Collaboration and Support: Collaborate with the vendor throughout the project, providing feedback and addressing any questions or concerns.
- Knowledge Transfer: Facilitate knowledge transfer from the vendor to NDA staff, ensuring a smooth transition and ongoing maintenance of security measures.

Note: The vendor selection process should adhere to the normal state procurement process for contracts of this size, ensuring transparency, fairness, and compliance with applicable regulations.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The primary desired outcome of this project is to enhance the Nevada Department of Agriculture's (NDA) cybersecurity posture by identifying and addressing critical vulnerabilities. This will be achieved through:

- Improved security controls: Implementing measures to strengthen NDA's security controls and align with NIST CSF best practices.
- Reduced risk of cyberattacks: Minimizing the likelihood of successful cyberattacks that could compromise NDA's operations or data.
- Enhanced data protection: Protecting sensitive data from unauthorized access, theft, or loss.
- Increased resilience: Enabling NDA to recover quickly from cyber incidents and minimize disruptions to services.
- Compliance with industry standards: Demonstrating NDA's commitment to cybersecurity best practices and meeting regulatory requirements.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
NDA understands this provision.

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☑ 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. 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.
The project is scalable to some extent. It can be expanded to include additional assessments or in-depth analysis of specific areas, such as network security or application security. However, reducing the scope of the project might compromise the effectiveness of the overall assessment.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89431

14. 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.
- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Cyber Security Risk Gap Assessment	Third-party cyber security risk gap assessment, based on NIST.	1	25,500.00	$ 25,500.00	The cost of the risk assessment is directly tied to the project's objectives. By conducting a comprehensive gap assessment against the NIST Cybersecurity Framework, the project aims to: Identify critical vulnerabilities: This information will allow NDA to prioritize mitigation efforts and allocate resources effectively. Develop a remediation plan: The assessment will inform the development of a targeted plan to address identified security gaps. Reduce risk: By understanding and addressing vulnerabilities, NDA can reduce the risk of cyberattacks and protect sensitive data. Therefore, the cost of the risk assessment is an investment in NDA's cybersecurity posture, enabling it to make informed decisions and take proactive measures to protect its operations.	While this project is a one-time assessment, NDA can leverage its outcomes to ensure long-term sustainability: Baseline for Future Assessments: The initial assessment will establish a baseline for future cybersecurity evaluations, enabling NDA to track progress and identify emerging risks. Inform Strategic Planning: The assessment results can inform NDA's overall cybersecurity strategy, guiding future investments and initiatives. Demonstrate Commitment: A successful assessment can demonstrate NDA's commitment to cybersecurity and facilitate the acquisition of future funding or resources. By utilizing the insights gained from this one-time assessment, NDA can lay a strong foundation for ongoing cybersecurity efforts and ensure the long-term protection of its critical infrastructure.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		1	**25,500.00**	**$ 25,500.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		

				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
				$	$			
			0	$ 0.00	$ 0.00			

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		0	$ 0.00	$ 0.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			

			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		0
Total		0	$ 0.00	$0.00		0

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	SON 2022 FINAL Single Audit Report
Travel Policy	☑	2.5_travel_pol_ada_final_signed
Payroll Policy	☑	NAC 284
Procurement Policy	☑	NRS 333
Milestones download template	☑	Milestones - NDA Cyber Security Risk Gap Assessment

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

Application ID: 483098

	Applicant Name	Nevada Department of Agriculture
	Project Name:	NDA Cyber Security Risk Gap Assessment
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Procurement Completed	3/31/2025
2	Project Initiation	4/1/2025
3	Phase 1 Complete - Document collection & analysis	4/25/2025
4	Phase 2 Complete - Initial Interviews & Compliance Check	5/9/2025
5	Phase 3 Complete - Gap Analysis	5/16/2025
6	Phase 4 Complete - Documentation & Second Round of Interviews	5/30/2025
7	Phase 5 Complete - Policy/Porcess Document Assessment	6/20/2025
8	Phase 6 Complete - Reporting and Closing	6/27/2025
9		
10		

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Nevada Department of Taxation

Taxation log and alert enhancements

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

$ 113,568.00 Requested

Submitted: 9/25/2024 10:48:27 AM (Pacific)

Project Contact
James Underwood
underwoodj@tax.state.nv.us
Tel: 775-684-2167

Additional Contacts
none entered

Nevada Department of Taxation

3850 Arrowhead Dr
Carson City, NV 89706
United States

Administrative Services Officer IV
Bonnie Long
blong@tax.state.nv.us

Telephone	775-684-2000
Fax	
Web	
EIN	88-6000022
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.

- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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 Question 12 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 purpose of this project is to hire a contractor to make improvements to Taxation's currently implemented logging system. The system ingests logs from various systems such as virtualization hosts, servers, routers, and firewalls. Alerts are configured based custom search queries to call attention to events that require follow-up by information security staff.

The system is built on free and open software. It has powerful search syntax, so it is easy to find exactly what you are looking for, even in terabytes of log data. One of the most important distinguishing points in favor of the system that Taxation uses is that it was designed as a powerful logging solution from the start, whereas other free and open source software has been adapted to logging. This system can receive structured logs and standard syslog directly from an application via the network protocol.

The agency has used the current logging system for several years and has built some important capabilities to help protect Taxation’s systems that process approximately $10 billion in annual revenue for state and local government entities. This grant will help improve protection of those systems.

The goals of the project are to:

1. Expand Taxation’s logging system implementation beyond one node
2. Streamline and optimize inputs into the logging system
3. Expand the footprint of data sources for inputs into the logging system
4. Expand and optimize alerts
5. Enable archiving of data beyond certain time period to ensure system efficiency
6. Document the system so that it can be maintained by existing Taxation staff
7. Document the implementation and share it with other agencies so that they may implement a similar system at a lower cost

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

This project will result in significant enhancements to the department's incident response capabilities by:

1. Creating and maintaining a more robust searchable database of logs
2. Providing relevant and timely alerts of events that may signal an incident
3. Enhancing root cause analysis

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

Implementing enhanced logging is a best practice in the preparation to protect state information systems, applications, and user accounts against cybersecurity risks and cybersecurity threats. Logs are vital to responding to a cybersecurity threat or incident.

7. 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.

Existing Taxation staff will work closely with a contracted Client Technologies Specialist for 6 months. Existing hardware will be used for compute and storage.

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

Staff believes that this project is highly likely to be successful due to current knowledge of the system. The major barrier for staff to complete this project is time and competing priorities.

The first desired outcome is to significantly enhance the protection of Taxation’s systems that process incoming revenue and distribute that revenue to state and local government entities.

The second desired outcome is to provide a documentation resource that can be shared with other state and local agencies so that they may implement a similar project

with a lower barrier to entry.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
I understand.

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- [ ] Yes
- [x] No

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), either on our own or as a condition of FY 2022 SLCGP
- [x] 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. 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, this project can be scaled down approximately 15% and be likely to achieve the desired outcome. The scaling would be in the number of contracted hours or the level of the contractor from 4 to 3.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89706

14. 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.
- [x] Build
- [ ] Sustain

15. 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
- [x] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Contractor	Client Technologies Specialist Level 4	1,040	109.20	$ 113,568.00	The contractor will directly work with existing staff to implement the project.	Existing staff has the capability to maintain the system once the project has been completed. Documentation developed by the contractor and existing staff will ensure supportability of the system.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		

					$		
					$		
					$		
					$		
					$		
		1,040			$		
			109.20	113,568.00			

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	$ 0.00	$ 0.00		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		0	$ 0.00	$ 0.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			

			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	2022 ACFR Report
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestones

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

Application ID: 482441

	Applicant Name	Nevada Department of Taxation
	Project Name:	Taxation log and alert enhancements
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Contractor hired	11/30/2024
2	Multinode system built & documented	12/31/2024
3	Input sources expanded and optimized	2/28/2025
4	Alerts expanded and optimized	4/30/2025
5	Archiving configured and operational	5/15/2025
6	All documentation completed	5/30/2025
7		
8		
9		
10		

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Nevada Department of Transportation - Cybersecurity

NDOT Security Awareness and Role Specific Training for Cybersecurity

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

$ 168,082.00 Requested

Submitted: 9/23/2024 1:42:34 PM (Pacific)

Project Contact
Rick Hays
rhays@dot.nv.gov
Tel: 7757724297

Additional Contacts
ChristopherJohnson@dot.nv.gov

Nevada Department of Transportation - Cybersecurity

1263 S Stewart St
Carson City, NV 89712
United States

Chief Accountant
Tiffany Smorra
TSmorra@dot.nv.gov

Telephone	7757724297
Fax	
Web	
EIN	Nevada Dep
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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.

- [x] 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.
- [x] 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.
- [x] 12. Leverage cybersecurity services offered by CISA. (See Question 12 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?

Focusing on Cybersecurity professional training that aligns with each cybersecurity team member's roles and responsibilities and aligns with their work role in the NICE Framework. - Train users to become more cyber aware and become less susceptible to social engineering, and phishing attacks. And it informs users on resources available in case of a data/cyber incident. This will be accomplished through purchasing user training from multiple sources.

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

It directly aligns by providing training for users.

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

NDOT employees will acquire cybersecurity awareness training to enhance their ability to detect and report security concerns and incidents. By training NDOT employees it will provide the backbone to create a proactive cyber secure environment. The CISA service that NDOT leverages is The Federal Virtual Training Environment (FedVTE). FedVTE is used to provide cybersecurity training to U.S. government personnel and veterans. Cybersecurity personnel need to monitor the network and all of its assets via an automated and non-auomated methodology, to ensure they understand not only the threats, but also the areas where the network and its assets are vulnerable, in order to have a full risk awareness.

7. 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.

The NDOT cyber security team, led by our Chief Information Security Officer (CISO), will obtain curated training courses that align with the Center for Internet Security (CIS) Assessment Control item 14.9 (Conduct Role-Specific Security Awareness and Skills Training). This obtained training will allow each trained NDOT Cybersecurity Team member to conduct distributed training to the rest of the NDOT Cybersecurity Team. This training will also allow for improved cybersecurity awareness and cyber hygiene.

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

Trained, aware, and cyber conscious users will better protect NDOT agency as a whole and prevent future cyber incidents.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.

M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)

No

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?

EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.

- [ ] Yes
- [x] No

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), either on our own or as a condition of FY 2022 SLCGP
- ☑ 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. 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, it can be expanded to cover multiple skill sets and reduced to cover basic security awareness and role based training needs.

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

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

89712

14. 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

15. 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

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

Each selection should have an accompanying item in the line item detail budget table on the next tab

- ☐ 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	$ 0.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		

			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		0	$ 0.00	$ 0.00				

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		0	$ 0.00	$ 0.00				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
Training Governance Risk and Compliance Analyst	Security skills and techniques you need to protect and secure network, endpoint, and cloud. Cybersecurity Governance, Risk, and Compliance. Incident Management Response.	3	$ 8,555.00	$ 25,665.00			
Training Governance Risk and Compliance A	Cybersecurity Governance, Risk, and Compliance. Incident Management Response.	1	$ 920.00	$ 920.00			
Training Deputy CISO-Treat Intelligence	Advanced Incident Response, Threat Hunting, and Digital Forensics	1	$ 7,925.00	$ 7,925.00			
Training Deputy CISO-Compliance Manager	Implementing and Auditing Security Controls. Cybersecurity Incident Management and Response.	1	$ 16,015.00	$ 16,015.00			
Training Deputy CISO-Security Architect	Cloud Security Architecture	1	$ 8,555.00	$ 8,555.00			
Training Deputy CISO-AI Governance and Architect	Applied Data Science and AI Machine Learning. AI security essentials for business.	1	$ 8,855.00	$ 8,855.00			
Training Deputy CISO-Physical Security	Physical Security Assessments, Designs, Applications, Implementations, and Integration	1	$ 725.00	$ 725.00			
Training Travel Costs	Costs Associated with Training Travel and Per Diem	1	$ 21,392.00	$ 21,392.00			

Training Deputy CISO - Security Architect	Cybersecurity Architecture	1	$ 6,150.00	$ 6,150.00		
Training Senior Software Design Security	Certified Secure Software Lifecycle Professional	1	$ 550.00	$ 550.00		
Training Network Security Architecture	Security Skills and Techniques to Protect a Secure Network, Endpoint, and Cloud	4	$ 5,000.00	$ 20,000.00		
Training IT Security Technician	Secure Network, Endpoint, and Cloud.Cybersecurity Incident Management and Response.	4	$ 8,555.00	$ 34,220.00		
Training Digital Forensics Professional	E-Discovery, Forensics Analysis and Reporting	2	$ 8,555.00	$ 17,110.00		
			$	$		
		22	**$ 101,752.00**	**$ 168,082.00**		**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	**$ 0.00**			**0**
Total		**0**	**$ 0.00**	**$0.00**			**0**

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	NDOT Audit
Travel Policy	☑	Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Milestones
		Capability Assessment

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

Application ID: 481287

	Applicant Name	Nevada Department of Transportation
	Project Name:	NDOT Security Awareness and Role based training
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Training Governance Risk and Compliance Analyst	Friday, November 28, 2025
2	Training Deputy Chief Information Security Officer - Threat Intelligence	Friday, November 28, 2025
3	Training Governance Risk and Compliance Analyst	Friday, November 28, 2025
4	Deputy Chief Information Officer - Compliance	Friday, November 28, 2025
5	Training Deputy Chief Information Security Officer - Security Architect	Friday, November 28, 2025
6	Deputy Chief Information Security Officer - AI Governance and Architecture	Friday, November 28, 2025
7	Training Deputy Chief Information Security Officer - Physcial Security	Friday, November 28, 2025
9	Training Information Technology Security Technician	Friday, November 28, 2025
10	Training Information Technology Security Technician	Friday, November 28, 2025
11	Training Digital Forensic Professional	Friday, November 28, 2025
12	Training Network Team	Friday, November 28, 2025
13	Training Senior Software Engineer Security	Friday, November 28, 2025

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Pahranagat Valley Volunteer Fire District

Ransomware Protected Backup

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

$ 10,800.00 Requested

Submitted: 9/27/2024 10:08:22 AM (Pacific)

Project Contact
Brittany Smallwood
bsmallwood@pvvfire.org
Tel: 7024160011

Additional Contacts
none entered

Pahranagat Valley Volunteer Fire District

655 Box Canyon Rd
PO BOX 540
Alamo, NV 89001
United States

Chariman
Mashall Davis
marshalldavis341@yahoo.com

Telephone	7757253644
Fax	7757253333
Web	www.pvvfire.org
EIN	880281542
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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.
- [x] Yes
- [ ] No

2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 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.
- [x] 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?
Protect Data from Ransomware by implementing Network Attached Storage (NAS) and a backup solution that copies the data offsite.

Backups play a crucial role in mitigating the impact of ransomware attacks.

1. Data Recovery
If ransomware encrypts our files, having a recent backup allows us to restore our data to a point before the attack, avoiding the need to pay the ransom.

2. Multiple Copies
Following the 3-2-1 backup rule (3 copies of your data, 2 on different media, 1 off-site) ensures that even if one backup is compromised, we have other copies to restore from.

3. Isolation
Keeping backups isolated from our main network (e.g., offline or in the cloud) prevents ransomware from reaching and encrypting our backup files.

4. Regular Backups
Frequent backups minimize data loss by ensuring that the most recent data is preserved. This means we can recover almost all our data even if an attack occurs.

5. Testing and Verification
Regularly testing and verifying your backups ensures they are functional and can be restored quickly in case of an attack.

6. Snapshot Technology
Some backup solutions offer snapshot technology, which captures the state of our data at specific points in time. This allows us to roll back to a clean state before the ransomware infection.

By implementing a robust backup strategy, we can significantly reduce the impact of ransomware and ensure your data remains safe and recoverable.

5. How does your project align with the objective selected in Question 2?
Enhancing the preparation, response, and resilience of information systems, applications, and user accounts against cybersecurity risks and threats, especially for state and local governments, involves several key strategies. Here's how backups can play a crucial role in this process:

1. Regular and Automated Backups
• Frequency: Implement regular, automated backups to ensure that data is consistently saved and up-to-date. This minimizes data loss in case of an attack.
• Testing: Regularly test backups to ensure they can be restored quickly and effectively.

2. Off-Site and Cloud Backups
• Isolation: Store backups off-site or in the cloud to isolate them from the main network. This prevents ransomware from reaching and encrypting backup files.
• Redundancy: Use multiple backup locations to ensure redundancy and availability.

3. Snapshot Technology
• Point-in-Time Recovery: Utilize snapshot technology to capture the state of your systems at specific points in time. This allows for quick recovery to a state before the ransomware attack.

4. Access Controls and Encryption
• Restricted Access: Implement strong access controls to limit who can access and modify backups. Use multi-factor authentication (MFA) for added security.
• Encryption: Encrypt backup data to protect it from unauthorized access and ensure its integrity.

5. Incident Response Planning
• Backup Integration: Integrate backup strategies into our incident response plan. Ensure that our team knows how to quickly restore data from backups in the event of a ransomware attack.
• Training: Regularly train staff on backup procedures and the importance of maintaining backup integrity.

6. Compliance and Best Practices
• Adherence to Standards: Follow industry standards and best practices for data backup and recovery. This includes the 3-2-1 backup rule (3 copies of data, 2 different media, 1 off-site).

• Regular Audits: Conduct regular audits of backup processes to ensure compliance and identify areas for improvement.

By implementing these strategies, we can significantly enhance our resilience against cybersecurity threats, ensuring that critical data and systems can be quickly restored in the event of an attack.

6. How does your project align with the program element(s) selected in Question 3?
Backups are a critical component in enhancing the preparation, response, and resilience of information systems, applications, and user accounts against cybersecurity risks and threats. Here's how they contribute to these goals:

1. Preparation
- Regular Backups: Implementing regular backups ensures that data is consistently saved and up-to-date, reducing the risk of significant data loss.
- Automated Processes: Automating backup processes minimizes human error and ensures that backups are performed consistently.

2. Response
- Quick Recovery: In the event of a cybersecurity incident, such as a ransomware attack, having recent backups allows for quick restoration of data, minimizing downtime.
- Incident Response Plans: Integrating backup strategies into incident response plans ensures that teams know how to quickly access and restore data from backups during an incident.

3. Resilience
- Data Integrity: Backups help maintain the integrity of data by providing a clean copy that can be restored if the primary data is compromised.
- Redundancy: Following best practices like the 3-2-1 backup rule (3 copies of data, 2 different media, 1 off-site) ensures that there are multiple copies of data available, even if one is compromised.

4. Continuity of Operations
- Disaster Recovery: Backups are essential for disaster recovery plans, ensuring that critical data and systems can be restored quickly to maintain operations.
- Exercises and Drills: Conducting regular exercises and drills to practice responding to cybersecurity incidents, including restoring from backups, helps ensure that teams are prepared and can respond effectively.

5. Compliance and Best Practices
- Adherence to Standards: Following industry standards and best practices for data backup and recovery ensures that state and local governments are prepared for cybersecurity threats.
- Regular Audits: Conducting regular audits of backup processes helps identify areas for improvement and ensures compliance with regulations.

By implementing robust backup strategies, we can enhance their ability to prepare for, respond to, and recover from cybersecurity incidents, ensuring the continuity of operations and the protection of critical data and systems.

7. 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.
There is an on-site engineer that will work with vendor's engineers remotely to implement this project.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcomes of a project focused on enhancing the preparation, response, and resilience of information systems, applications, and user accounts against cybersecurity risks and threats include:

1. Improved Data Security
- Reduced Risk of Data Loss: Ensuring that critical data is regularly backed up and can be quickly restored in the event of a cybersecurity incident.
- Enhanced Data Integrity: Maintaining the integrity of data through secure backup practices and regular testing.

2. Increased Operational Resilience
- Continuity of Operations: Ensuring that government services can continue with minimal disruption during and after a cybersecurity incident.
- Quick Recovery: Reducing downtime by having efficient backup and recovery processes in place.

3. Effective Incident Response
- Preparedness: Having a well-defined incident response plan that includes backup and recovery procedures.
- Training and Drills: Conducting regular exercises to practice responding to cybersecurity incidents, ensuring that staff are prepared and confident in their roles. We are a fire department and understand the need for training and preparedness.

4. Compliance and Best Practices
- Adherence to Standards: Meeting industry standards and regulatory requirements for data backup and cybersecurity.
- Regular Audits: Conducting audits to ensure compliance and identify areas for improvement.

5. Enhanced Collaboration and Funding
- Resource Sharing: Collaborating with other government entities and cybersecurity organizations to share resources and best practices.
- Securing Grants: Leveraging state and federal grants to fund cybersecurity initiatives, including robust backup solutions.

6. Public Trust and Confidence
- Transparency: Demonstrating a commitment to protecting data and maintaining operations, which can enhance public trust and confidence in government services.

By achieving these outcomes, we can better protect our patient information systems, ensure the continuity of critical services, and enhance our overall cybersecurity posture.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☑ 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. 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.
The project is scalable to users in the same network.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89001

14. 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

15. 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

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab

- ☐ 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	**$ 0.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	**$ 0.00**	**$ 0.00**		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Hardened Backup	Hardened Backup Server	1	$ 9,000.00	$ 9,000.00	The is the servers that will store PVVFD data	Since we have the hardware the PVVFD will be able to pay for renewal licenses.	Hardware, Computer, Inte	04HW-01-INHW
Installation Cost	Installer	10	$ 180.00	$ 1,800.00				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		11	**$ 9,180.00**	**$ 10,800.00**				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	**$ 0.00**			**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	**$ 0.00**			**0**
Total		**0**	**$ 0.00**	**$0.00**			**0**

Document Uploads *top*

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

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

Application ID: 482027

	Applicant Name	PVVFD
	Project Name:	Backup
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Grant Writing and Approval	15-Oct
2	**Project Planning**:	15-Nov
3	**Vendor Selection**	1-Dec
4	**Preparation:**	10-Dec
5	**Hardware and Software Procurement**	31-Dec
6	**Configuration and Setup**	15-Jan
7	**Training and Documentation**	20-Jan
8	**Implementation and Go-Live**	1-Feb
9	**Monitoring and Maintenance**	15-Feb
10	Project Review and Closure	1-Mar

*Please add additional rows as necessary for your project

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Reno-Tahoe Airport Authority

Comprehensive Firewall Modernization and Enhancement

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

$ 176,228.74 Requested

Submitted: 9/27/2024 3:56:14 PM (Pacific)

Project Contact
Arthur Rempp
arempp@renoairport.com
Tel: 775-328-6684

Additional Contacts
none entered

Reno-Tahoe Airport Authority

2770 Vassar St
Reno, NV 89502
United States

Chief Finance & Administrative Officer
Randall Carlton
rcarlton@renoairport.com

Telephone	775-328-6684
Fax	
Web	renoairport.com
EIN	88-0156921
UEI	Z12LXSDCFMN4
SAM Expires	1/21/2025

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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.
- [x] 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 Question 12 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 Reno-Tahoe Airport Authority aims to replace the current firewall with a next-generation firewall to enhance cybersecurity and future-proof our network against evolving threats.

This project will improve cybersecurity protection in the following ways:
• Strengthen Cybersecurity: We want to implement advanced threat protection, leveraging machine learning to detect and block malware, ransomware, and phishing attempts in real-time. This will ensure better protection against both known and unknown threats.
• Improve Network Visibility: We intend to gain deeper insights into all network traffic, allowing us to identify and control applications, users, and content. This enhanced visibility will help us spot irregular activities faster and prevent potential security breaches.
• Utilize Advanced Threat Intelligence: By switching to a next-generation firewall, we can integrate global threat intelligence that constantly updates and responds to new cyber threats. This proactive approach is most effective. Newer policy creation wizards use AIOps to continuously recommend best practices on any change, effectively providing real-time guardrails to the user.
• Implement Granular Network Controls: We want to implement Zero-Trust security policies that allow more precise control over who or what accesses our network. Segmentation will help protect sensitive data by minimizing lateral movement within the network.
• Automate & Simplify Security Management: Our goal is to streamline firewall management, using automated features to deploy updates and enforce policies. This will reduce manual effort, minimize human error, and improve response times.
• Ensure Scalability & Future Protection: As we grow, we need a firewall solution that can scale with us. Newer flexible architecture will allow us to expand without frequent hardware upgrades, ensuring long-term cybersecurity.
In summary, our objective is to improve the security, efficiency, and scalability of our network by upgrading to a next-generation firewall, providing our agency with robust protection against modern cyber threats.

5. How does your project align with the objective selected in Question 2?
Our project strongly supports Objective 3: Implement security protections commensurate with risk by focusing on a critical upgrade to our firewall infrastructure.

This upgrade is not just a security enhancement, but a foundational step in transforming the Transportation sector to meet the demands of a rapidly evolving threat landscape. The Transportation sector, a key component of national infrastructure, faces unprecedented cyber risks, and our project seeks to address these with precision and urgency. Because Reno-Tahoe International Airport (RNO) plays a significant role in driving the local economy, with an annual economic impact of around $3.6 billion, cybersecurity is a major concern. This figure represents approximately 8% of northern Nevada's total economic output. The airport directly supports over 6,300 jobs and indirectly contributes to over 17,500 more, accounting for about 6% of regional employment.

Key benefits of this project include:
• Strengthened Defense Against Emerging Threats: The updated firewall will offer enhanced protection against a broad spectrum of cybersecurity risks, particularly those increasingly targeting transportation systems.
• Secure Integration of New Technologies: With this upgrade, we will be able to safely deploy advanced technologies—such as automated systems, IoT devices, and connected infrastructure—that will drive efficiency and innovation without compromising security.
• Risk Mitigation Tailored to Critical Infrastructure: By implementing this firewall upgrade, we ensure that our security protections are precisely scaled to meet the specific and growing risks associated with the Transportation sector.
• Proactive Response to Cyber Threats: Rather than reacting to incidents, this project puts us ahead of potential risks, ensuring our infrastructure can withstand new and evolving cyber threats.

By fortifying our digital defenses, we enable the safe and secure integration of new technologies while reducing vulnerabilities across the board. This aligns directly with the objective of implementing security measures that match the complexity and scale of today's risks.

6. How does your project align with the program element(s) selected in Question 3?
By upgrading our firewall infrastructure, we significantly improve the visibility and control over network activities transiting to and from our critical systems. This enhancement is vital for detecting and mitigating cybersecurity threats that could impact the airport's operations and, by extension, the regional economy.

Key ways our project supports this program element include:
• Enhanced Network Monitoring: The upgraded firewall provides advanced real-time monitoring capabilities, allowing us to closely observe network traffic patterns and identify unusual or suspicious activities that may indicate potential cybersecurity risks.
• Improved Auditing Capabilities: With comprehensive logging and reporting features, we can conduct thorough audits of all network activities. This ensures compliance with security policies and helps in pinpointing vulnerabilities within our information systems.
• Advanced Threat Detection and Prevention: The new firewall includes next-generation security features that can detect and block malicious traffic, protecting our systems and user accounts from cyber-attacks aimed at the transportation sector.
• Secure Management of User Accounts: By closely tracking access to applications and systems, we ensure that only authorized personnel interact with sensitive data, thereby preventing unauthorized access and potential security breaches.
By implementing these measures, our project not only aligns with but actively advances the program element's objective of safeguarding government-operated information systems through effective monitoring, auditing, and tracking. This is especially crucial in the transportation sector, where the security and integrity of information systems and data are essential for safe and efficient operations at RNO, a key economic driver in northern Nevada.

7. 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.
The RTAA IT team will engage and work closely with vendors to configure and implement the new next-generation firewall solution. This will provide the RTAA IT team access to vendor expertise and experience that will shorten the implementation timeline and knowledge to support the firewall in the future.

Implementation steps:
• Phase 1: Planning & Design – We'll assess the existing network to plan the best configuration for the new firewall, ensuring minimal disruption. Planning will be with the RTAA IT team and the vendor implementation teams.
• Phase 2: Deployment – The new firewall will be installed alongside the current firewall to allow a smooth transition. This will continue to be a collaborative effort between the RTAA team and the vendor teams.
• Phase 3: Testing & Optimization – We will rigorously test and fine-tune the firewall to maximize performance and security.
• Phase 4: Monitoring & Training – Continuous monitoring will keep our network secure, while staff will be trained to manage and troubleshoot the new system. With the experience of configuration and implementation, the RTAA team will be in a good position to monitor and optimize the firewall in the future. Continuing training will occur for new staff as necessary through a combination of peer-to-peer learning and formal training as needed from appropriate vendors.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome of this project is to upgrade the current firewall to a next-generation firewall. This will enhance the agency's overall cybersecurity by implementing advanced threat prevention, real-time monitoring, and zero-trust network segmentation. Additionally, the firewall upgrade aims to improve network visibility, streamline security management through automation, and provide scalability to support future growth. These outcomes will ensure stronger protection against modern cyber threats and create a more secure environment for sensitive data handling.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
Understood

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☑ 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. 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, this project is scalable and can be adapted to the needs of the agency. The scope of the firewall upgrade can be reduced by initially deploying only essential features, such as basic threat detection and firewall functions, while deferring more advanced configurations like full network segmentation or AI-powered threat intelligence for future phases. On the other hand, the project can be expanded by adding more comprehensive security layers, such as multi-factor authentication, deep packet inspection, or integration with cloud security platforms as the agency grows. Most next-generation firewall's modular architecture allows for seamless expansion without significant hardware upgrades, making it adaptable to both current needs and future demands.

This flexibility ensures that the agency can scale the solution in line with budget, operational growth, and emerging cybersecurity threats.

Our recommendation is not to reduce the scoped solution.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89502

14. 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

15. 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

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- ☐ 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		

					$			
					$			
					$			
					$			
					$			
					$			
					$			
					$			
					$			
					$			
		0	**0.00**	**$ 0.00**				

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	**$ 0.00**	**$ 0.00**		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Network Firewall	Hardware	2	$ 29,030.20	$ 58,060.40	Required hardware	One-time cost	Firewall, Network	05NP-00-FWAL
Lab Unit Firewall	Hardware	1	$ 379.50	$ 379.50	Required hardware	One-time cost	Firewall, Network	05NP-00-FWAL
Advanced Threat Prevention	Software	2	$ 24,816.32	$ 49,632.64	Required software for the protection components	Will become a budgeted item	Firewall, Network	05NP-00-FWAL
Lab Unit Service	Software	1	$ 83.95	$ 83.95	Software service support	Will become a budgeted item	Firewall, Network	05NP-00-FWAL
Support per firewall	Hardware maintenance	2	$ 27,220.50	$ 54,441.00	Maintenance support	Will become a budgeted item	Firewall, Network	05NP-00-FWAL
Configuration and implementation of Firewall	Services	1	$ 13,631.25	$ 13,631.25	Configuration and implmentation services	One-time cost	Firewall, Network	05NP-00-FWAL
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		9	**$ 95,161.72**	**$ 176,228.74**				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
			$	$			
			$	$			
			$	$			
			$	$			

			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		0	$ 0.00	$ 0.00				0

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

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

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

Application ID: 483106

	Applicant Name	City of Reno
	Project Name:	Cloud Backup & On Premise Backup Assessment
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	Project RFP	1/1/2025
2	On Premise Assessment Implementation	3/1/2025
3	Cloud Backup Implementation	3/1/2025
4	Security Appliance Configuration	3/1/2025
5	On Premise Assessment Review	4/1/2025
6	Cloud Backup Completion	4/15/2025
7	Security Appliance Complete	3/15/2025
8	On Premise Configuration Changes	4/7/2025
9	On Premise Complete	5/1/2025
10		

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

University of Nevada, Las Vegas

Planning for Statewide SOC / NV-ISAC

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

$ 391,000.00 Requested

Submitted: 9/26/2024 3:50:44 PM (Pacific)

Project Contact
Vito Rocco
vito.rocco@unlv.edu
Tel: 7028950400

Additional Contacts
kivanc.oner@unlv.edu

University of Nevada, Las Vegas

4505 S Maryland Pkwy
Las Vegas, NV 89154
United States

Chief Financial Officer
Casey Wyman
casey.wyman@unlv.edu

Telephone	7028950400
Fax	
Web	unlv.edu
EIN	88-6000024
UEI	
SAM Expires	

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 SLCGP. Please select the objective with which your project most closely aligns.
- [x] 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.

- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 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.
- [x] 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 University of Nevada, Las Vegas (UNLV) seeks a planning grant to support the development of a statewide Security Operations Center (SOC) initiative in collaboration with the Nevada State Office of the CIO (OCIO) and the Office of Cyber Defense Coordination (OCDC). This initiative aims to establish a SOC that provides cybersecurity monitoring, threat detection, and response services to underserved municipalities across Nevada. The focus of this project is on planning and laying the groundwork for the future SOC, ensuring that smaller, resource-limited local governments can access critical cybersecurity resources.

The requested $391,000 will be used to fund key planning activities, including:

Conducting feasibility studies to define the SOC's structure, operations, and service offerings.
Engaging external consultants to design the SOC's operational framework, governance, and staffing models.
Collaborating with state agencies and municipalities to assess needs and identify priority areas for cybersecurity support.
Developing key documentation such as organizational charters, operational guidelines, and staffing plans.
Identifying required technology and tools for the SOC and estimating associated costs.
Establishing a plan for a Nevada Information Sharing and Analysis Center (ISAC) to enhance real-time threat intelligence sharing between state and local agencies.
This planning project is critical because many Nevada municipalities lack the resources needed to protect against increasingly sophisticated cyber threats. A centralized SOC would address these gaps by providing the necessary expertise and infrastructure to safeguard digital assets across the state. By conducting this planning effort, we can ensure that the SOC is designed in a way that aligns with best practices while being tailored to the unique needs of Nevada's local governments.

Additionally, this initiative will include UNLV students as part of the SOC workforce, allowing them to gain valuable, hands-on experience in cybersecurity. This will not only help address Nevada's immediate cybersecurity challenges but also contribute to the development of a strong cybersecurity workforce within the state, helping to close the talent gap in this critical field.

How the Project Improves Cybersecurity Protection:

Strategic Planning: By carefully planning the SOC's structure, services, and governance, this project will lay the foundation for a sustainable cybersecurity operation that can support municipalities statewide.
Workforce Development: Involving UNLV students will create a long-term pipeline of trained cybersecurity professionals equipped to support Nevada's cybersecurity efforts both now and in the future.
Collaboration and Intelligence Sharing: Planning for the Nevada ISAC will facilitate improved coordination and intelligence sharing across state and local governments, enhancing Nevada's ability to anticipate and respond to cyber threats.

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

Our project aligns with Objective 1: Develop and establish appropriate governance structures by focusing on the foundational planning necessary to establish a statewide Security Operations Center (SOC) and a Nevada Information Sharing and Analysis Center (ISAC). The primary goal of this planning effort is to create governance frameworks, operational plans, and structures that will enhance Nevada's cybersecurity incident response and continuity of operations capabilities.

This project will:

Develop organizational charters, governance models, and operational guidelines for the SOC.

Establish collaborative structures between state agencies, local governments, and municipalities to ensure coordinated cybersecurity efforts across Nevada.

Design the SOC's incident response protocols, continuity of operations plans, and mechanisms for efficient threat detection and response.

Plan for the creation of the Nevada ISAC, which will facilitate real-time cyber intelligence sharing and collaboration across the state.

By building these governance and operational frameworks, this project ensures that Nevada's local governments and municipalities, many of which are currently underserved in terms of cybersecurity resources, will have the capability to respond to incidents effectively and maintain resilience against evolving cyber threats. This approach aligns directly with the goal of strengthening governance structures to improve incident response and operational continuity across the state.

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

1. Manage, monitor, and track information systems:
The planning for the statewide SOC will focus on defining the processes and structures to manage, monitor, and track information systems and user accounts for municipalities across Nevada. The goal is to provide smaller, underserved governments with the necessary cybersecurity infrastructure to protect their digital assets.

3. Enhance preparation, response, and resilience against cybersecurity risks and threats:

The project will develop strategies and operational frameworks that enhance the state's ability to respond to and recover from cyber incidents. By planning for a centralized SOC, the state can ensure that all local governments are better prepared and more resilient in the face of growing cybersecurity threats.

5. Ensure best practices and methodologies to enhance cybersecurity:
Throughout the planning phase, we will focus on incorporating nationally recognized cybersecurity best practices. This ensures that the SOC and its services will help local governments improve their security posture, aligning with best practices recommended by CISA and other cybersecurity authorities.

7. Ensure continuity of operations:
A key part of this planning project is to ensure that the SOC will support continuity of operations for municipalities during a cyber incident. This will include developing incident response protocols and continuity plans to ensure that essential services can continue to operate during and after an attack.

8. Use the NICE Workforce Framework to enhance the cybersecurity workforce:
This project will integrate the NICE Workforce Framework to guide the recruitment, training, and retention of student workers who will staff the SOC. By aligning with this framework, we ensure that students are developing the necessary knowledge, skills, and abilities to fill critical cybersecurity roles in Nevada.

11. Enhance capabilities to share cyber threat indicators and related information:
The project includes planning for the establishment of a Nevada ISAC, which will enable real-time sharing of cyber threat intelligence between state and local entities. This capability is essential for enabling proactive threat mitigation across the state's municipal systems.

14. Develop and coordinate strategies to address cybersecurity risks:
This planning effort will involve coordination with local governments and key stakeholders to ensure that the SOC is developed with a comprehensive understanding of the cybersecurity risks facing Nevada. The project will lay the groundwork for long-term strategies that address these risks in a coordinated and sustainable way.

Through careful planning and alignment with these program elements, the project will establish the necessary governance and operational structures for a sustainable, effective statewide SOC.

7. 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.
The proposed project will be implemented through a collaborative effort between the University of Nevada, Las Vegas (UNLV), the Nevada State Office of the CIO (OCIO), the Office of Cyber Defense Coordination (OCDC), external consultants, and UNLV students. The key focus of this planning project is to ensure the development of a sustainable framework for a statewide Security Operations Center (SOC) and Information Sharing and Analysis Center (ISAC) that serves Nevada's municipalities.

Key Roles and Responsibilities:
Project Lead:

UNLV CISO: The UNLV Chief Information Security Officer (CISO) will serve as the primary lead and project manager, responsible for coordinating efforts between UNLV, the OCIO, and OCDC. The CISO will oversee all aspects of the project to ensure alignment with both university and state cybersecurity objectives.

Collaboration and Governance:

OCIO and OCDC Representatives: These stakeholders will provide strategic guidance throughout the project. They will help shape the scope and direction of the SOC, ensuring that the structure and services meet the needs of Nevada's municipalities.
Cybersecurity Planning Committee: A committee comprised of members from state and local governments will be established to provide ongoing guidance and feedback. The committee will be responsible for ensuring that the planning aligns with statewide priorities and addresses the unique challenges faced by smaller municipalities.

External Support:

Cybersecurity Consultants: External consultants will be engaged to assist in designing the SOC's governance and operational frameworks. They will conduct feasibility studies, identify cybersecurity gaps, and recommend best practices for the SOC's structure and future operations.
Technology Advisors: Specialists in cybersecurity technology will help identify the necessary tools and platforms for the SOC. They will assess the technological requirements and estimate the costs for future implementation phases.

UNLV Faculty and Students:

Project Coordinator: A project coordinator will be appointed from UNLV to handle daily operations, facilitate meetings, and manage the project timeline.
UNLV Faculty: Faculty members from the university's cybersecurity program will contribute expertise in designing the student workforce model. Their involvement ensures that the SOC will effectively integrate student workers, providing them with valuable hands-on experience.
UNLV Students: Students will be involved in research and assessments as part of their academic learning. This hands-on experience ensures the SOC planning incorporates a strong focus on workforce development.

8. Describe, in a few sentences, the desired outcome(s) of your project.
The desired outcome of this project is to develop a comprehensive plan and governance structure for a statewide Security Operations Center (SOC) that serves Nevada's municipalities. This plan will outline the SOC's operational framework, staffing models, and necessary technologies, while also establishing a Nevada Information Sharing and Analysis Center (ISAC) for real-time threat intelligence sharing. Additionally, the project will create a framework for a sustainable workforce development pathway by integrating UNLV students into the SOC, equipping them with hands-on experience to address Nevada's growing cybersecurity workforce needs.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
I understand that M&A costs are not being awarded for this grant.

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☑ 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. 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, this project is highly scalable. The initial planning for the statewide SOC can be expanded to cover more municipalities or reduced to focus on high-priority regions, such as rural communities in Nevada, based on available resources. The scope of services offered by the SOC, such as incident response, threat monitoring, and intelligence sharing, can also be adjusted depending on the state's needs and budget. Additionally, the integration of UNLV students can be scaled, with more students involved as the SOC grows or fewer during the initial stages. The technology and staffing plans can be modified to fit varying levels of funding and future growth, making the project flexible and adaptable.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89154

14. 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.
- [x] Build
- [ ] Sustain

15. 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.
- [x] Yes
- [ ] No

16. Please select all applicable planning, organization, equipment, training, and exercise (POETE) elements for which funding is being sought for this project.
Each selection should have an accompanying item in the line item detail budget table on the next tab
- [x] Planning - Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
- [x] Organization - Individual teams, an overall organizational structure, and leadership at each level in the structure
- [x] Equipment - Equipment, supplies, and systems that comply with relevant standards
- [x] 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Planning Consultant Services	Engage external consultants to conduct assessments, feasibility studies, and provide recommendations for SOC design and governance.	200	200.00	$ 40,000.00	This cost covers external expertise to help design the governance framework, incident response plans, and structure for the statewide SOC, including the analysis of cybersecurity needs in municipalities.	This is a one time cost and would not need sustaining.
Cybersecurity Planning Committee	Costs associated with convening the Cybersecurity Planning Committee, including meeting facilitation, travel expenses for committee members, and documentation.	10	1,000.00	$ 10,000.00	This funding ensures the committee has resources to guide the SOC planning process.	If funding is reduced, virtual meetings would be prioritized to reduce costs.
Technology Needs Assessment	Consultant-led assessment to identify necessary tools, software, and hardware for the future SOC.	1	50,000.00	$ 50,000.00	This cost covers a comprehensive review of technology needs, ensuring the SOC will be equipped with the right tools when implemented in future phases.	This is a one time cost and would not need sustaining.
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		211	**51,200.00**	**$ 100,000.00**		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
Full-Time Project Coordinator	Full-time coordinator responsible for overseeing the planning process, facilitating meetings, and managing the project timeline and resources.	1	$ 100,000.00	$ 100,000.00	This coordinator will manage daily project activities, ensuring that the project remains on track and that stakeholders are effectively engaged.	Once the statewide SOC is established and budgeted for by the state of NV, the intent would be for this salary to fall under that budget.
SOC Organizational Development Consultant	Consultant to assist in designing the SOC's organizational structure, staffing models, and leadership roles.	150	$ 200.00	$ 30,000.00	This cost will help develop the leadership framework, chain of command, and role definitions for the SOC's professional staff and student workers.	This is a one time cost and would not need sustaining.
UNLV Faculty and Student Involvement	Costs associated with faculty oversight and student research on SOC planning and workforce integration, including stipends.	10	$ 5,000.00	$ 50,000.00	This covers faculty time and student involvement to ensure the SOC plan integrates a strong educational component, preparing students for real-world SOC roles.	If funding is reduced, the number of student teams can be scaled down, focusing on key tasks.

Student Workers	Part-time student workers (20 hours per week) to support the planning process through research, analysis, and administrative tasks.	5,200	$ 17.50	$ 91,000.00	Students will support various planning activities, gaining valuable hands-on experience while contributing to the development of the SOC. Calculated 5 students @ 52 weeks.	If funding is reduced, fewer student workers will be hired, or their hours will be adjusted according to budget constraints. It is also the intent that the statewide SOC budget (once established) may support some of these costs.
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		5,361	**$ 105,217.50**	**$ 271,000.00**		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Student Worker Laptops	Computing resources to support the student workers working on the project	5	$ 2,000.00	$ 10,000.00	Laptops provide necessary tools for student workers to engage in project activities.	UNLV could use surplus equipment to meet this need.	Hardware, Computer, Integ	04HW-01-INHW
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		5	**$ 2,000.00**	**$ 10,000.00**				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
Student Training	Provide 5 student worker training sessions in tools used for planning and execution of the SOC/ NV-ISAC operations.	5	$ 2,000.00	$ 10,000.00	Training sessions ensure student workers are well-prepared for SOC roles.	Training would need to be reduced. The intent is for this item to become part of the statewide SOC budget once established.	yes
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		5	**$ 2,000.00**	**$ 10,000.00**			**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	$ 0.00	$ 0.00			0
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	A133 Audit UNLV
Travel Policy	☑	Travel Information UNLV
Payroll Policy	☑	UNLV Comp and Class
Procurement Policy	☑	Procurement Policy NSHE BoR
Milestones download template	☑	UNLV Milestones for Grant

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

Application ID: 482843

Applicant Name	University of Nevada, Las Vegas	
Project Name:	Planning for Statewide SOC / NV-ISAC	
Project Funding Stream:	FY 2023 SLCGP	

	Milestone Description*	Date of Expected Completion	Description
1	Hire Project Coordinator & Student Workers	Month 2	Recruit and onboard a full-time project coordinator to manage day-to-day operations and ensure project milestones are met.
2	Establish Cybersecurity Planning Committee	Month 3	Form the Cybersecurity Planning Committee with representatives from UNLV, OCIO, OCDC, and local governments to guide the planning process.
3	Engage External Consultants for SOC and ISAC Feasibility Assessment	Month 4	Contract external consultants to conduct a feasibility study for the SOC and ISAC development, including governance and operational frameworks.
4	Complete Initial Cybersecurity Needs Assessment for Nevada Municipalities	Month 6	Analyze cybersecurity needs of municipalities to identify key areas where the SOC can provide services.
5	Draft Governance and Operational Framework for SOC	Month 8	Finalize the initial governance and operational framework for the SOC, including leadership structure, staffing models, and service offerings.
6	Develop Initial Plan for Nevada ISAC	Month 9	Outline the framework for the Nevada Information Sharing and Analysis Center (ISAC), detailing its role in sharing cyber threat intelligence.
7	Identify and Estimate Costs for SOC Technology Needs	Month 10	Complete the technology needs assessment and provide estimates for necessary tools, software, and infrastructure for future SOC implementation.
8	Review and Finalize SOC and ISAC Planning Documents	Month 12	Compile and finalize all planning documents, including governance frameworks, operational guidelines, and technology assessments.
9			
10			

*Please add additional rows as necessary for your project

Powered by ZoomGrants™ and

Nevada Office of the Military, Division of Emergency Management

FFY 2023 State and Local Cybersecurity Grant Program (SLCGP)
Deadline: 9/27/2024

Washoe County Sheriff's Office

Northern Nevada Cyber Center

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

$ 297,312.52 Requested

Submitted: 9/25/2024 2:15:49 PM (Pacific)

Project Contact
Rebecca DiMaggio
SOGrants@washoecounty.us
Tel: 7753283013

Additional Contacts
none entered

Washoe County Sheriff's Office

911 Parr Blvd
Reno, NV 89512
United States

Sheriff
Darin Balaam
sogrants@washoecounty.us

Telephone 7753283013
Fax
Web
EIN 88-6000138
UEI LJCKY7DLT898
SAM Expires 10/19/2024

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.
- [x] 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).
- [x] 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.
- [x] 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. 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 Division of Emergency Management (DEM) 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.
- [x] 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.
- [x] I attest that funding for this project does not currently exist within our agency's budget

6. Due to a cost share waiver for FY 2023 SLCGP, there is no cost share for this grant.
- [x] 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, DEM is unable to issue a grant. Subgrantees may not pass through or subgrant funds to other agencies/organizations.
- [x] 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
- [x] No

2. There are four (4) objectives for FY 2023 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.
- [x] 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.
- [x] 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.
- [x] 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.
- [x] 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.

- [x] 5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity.
- [x] 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.
- [x] 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.
- [x] 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 Question 12 for further details on these services.)
- [x] 13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.
- [x] 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.
- [x] 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?

Training Requests:
1. Course – Performing a Cybersecurity Risk Assessment:
• For the manager to perform risk assessments for compliance and audits.
2. Course – Foundations: Computers, Technology, & Security:
• For two members to build fundamental cybersecurity knowledge, covering basic to intermediate concepts.
3. Course – Introduction to Cyber Security:
• For one member to cover a broad spectrum of cybersecurity topics including mobile device security, IoT, AI, authentication, authorization, cryptographic processes, network attacks, and more.
4. Course – Security Essentials – Network, Endpoint, and Cloud:
• For one member to cover essential skills for defending systems and networks.
5. Course - Practical Open-Source Intelligence (OSINT):
• For three expert members to cover OSINT research and investigations for law enforcement and private sector businesses.
6. Course – Reverse-Engineering Malware: Malware Analysis Tools and Techniques:
• For three expert members to learn malware analysis tools and techniques to examine malicious programs that target and infect Windows systems.
Benefits of Training:
• Bolster knowledge and skills to address cybersecurity risks.
• Implement continuous vulnerability assessments and threat mitigation.
• Increase knowledge of adversary tools and tactics.
• Adopt best practices to enhance cybersecurity.
Equipment Requests:
1. Cellebrite Software Licenses:
• Inseyets: A digital forensics solution for extracting, decoding, reviewing, managing, and triaging digital equipment.
• Inseyets Unlocks: Allows access to locked digital devices.
• Guardian: A digital evidence management system for secure evidence sharing and management.
Benefits of Cellebrite Software:
• Monitor, audit, and track activity on digital devices.
• Enhance the resilience of information systems against risks.
• Provide data encryption for data at rest and in transit.
• Enhance capabilities to share cyber threat information between state and local governments.
• Ensure access to services and programs in rural areas.
UPS Replacement Request:
• Uninterruptible Power Solution (UPS) Replacement:
The current UPS is over a decade old, failing frequently, and needs replacement to prevent unnecessary server room access and hardware degradation.
Benefits of UPS Replacement:
• Enhance resilience against cybersecurity risks.
• Mitigate risks to critical infrastructure and information systems.
• Ensure system reconstitution (backups).
This comprehensive request for training, equipment, and UPS replacement will significantly enhance the Cyber Center's capabilities to address and mitigate cybersecurity threats and ensure the security and resilience of critical infrastructure in Northern Nevada.

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

This project aligns with the primary federal grant objectives of (#4) training personnel in cybersecurity according to their responsibilities, and (#3) implementing risk-based security measures.

Primary Objective: Cybersecurity Training

• Cybersecurity Risk Assessment: Trains the manager to identify and mitigate risks for compliance.
• Foundations of Computers & Security: Provides essential knowledge for two members.
• Introduction to Cybersecurity: Teaches one member key topics like network attacks and cryptography.
• Security Essentials: Covers network, endpoint, and cloud defense skills.
• OSINT Training: Equips three members with advanced investigation skills.
• Malware Analysis: Teaches three members how to reverse-engineer malware.

The training enhances personnel's ability to assess and address cybersecurity threats effectively.

Secondary Objective: Risk-Based Security Protections

• Cellebrite Tools: Provides digital forensics capabilities for locked devices, boosting threat mitigation.
• Guardian: Streamlines evidence management and reporting.
• UPS Replacement: Ensures continuous power to the Cyber Center's server, reducing risk of data loss.

Together, the training and security tools ensure the Cyber Center can effectively prevent and respond to cybersecurity threats.

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

The project aligns with the selected program elements as follows:
2. Monitor, audit, and track network traffic and activity:
Cellebrite Software: Allows the Cyber Center to monitor, audit, and track digital devices and activity, ensuring comprehensive oversight of network traffic and user activities.
3. Enhance preparation, response, and resilience:
Training Courses: Equip personnel with skills to respond to cybersecurity threats.
Cellebrite Software and UPS Replacement: Improve system resilience and response capabilities.
4. Continuous cybersecurity vulnerability assessments and threat mitigation:
Training in Risk Assessment (LDR419): Helps the manager implement continuous vulnerability assessments.
Ongoing Training: Ensures personnel are updated on the latest threat mitigation practices.
5. Adopt and use best practices and methodologies:
Training: Ensures the adoption of industry best practices and methodologies in cybersecurity.
6. Promote safe, recognizable, and trustworthy online services:
Cellebrite Guardian: Enhances secure evidence management, promoting trust in online services provided by the cyber center.
8. Use NICE Framework to enhance the cybersecurity workforce:
Comprehensive Training Programs: Address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.
11. Enhance capabilities to share cyber threat indicators and related information:
Cellebrite Guardian: Facilitates secure sharing of cyber threat information between state and local governments.
13. IT and operational technology modernization cybersecurity review process:
Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives.

14. Develop and coordinate strategies to address cybersecurity risks and threats:
Collaborative Training and Tools: Develop strategies involving local and state governments, informed by continuous training and advanced tools.
15. Ensure access and participation by rural areas:
Cellebrite Software and Training: Extend cybersecurity services and programs to rural areas, ensuring equitable access.
This comprehensive approach ensures that the cyber center meets multiple program elements, enhancing overall cybersecurity preparedness and response capabilities for northern Nevada.

7. 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.
Training Implementation:
Members of the Northern Nevada Cyber Center will receive the training. Specific courses include:
Course: For the manager to perform cybersecurity risk assessments.
Course: For two members to build foundational cybersecurity knowledge.
Course: For one member to cover intermediate cybersecurity topics.
Course: For one member to learn essential system defense skills.
Course: For three experts to learn practical OSINT techniques.
Course: For three experts to learn practical malware examination tools and techniques.
Equipment Utilization:
Cellebrite Products:
Inseyets and Guardian will be used by the Northern Nevada Cyber Center members.
Inseyets: For extracting, decoding, reviewing, managing, and triaging digital equipment.
Guardian: For secure digital evidence management, sharing, and streamlining forensic processes.
UPS Replacement:
Installation:
Washoe County Information Technology (IT) technicians will install the new UPS.
This replacement is necessary due to the current UPS's age and frequent failures, which compromise server security and functionality.
Project Management:
Grant Management: WCSO Project Manager Cyber Sgt, Fiscal Grant Coordinator
Process to Accomplish the Project:
Planning Phase:
Coordination with training vendor: Schedule and organize the training sessions.
Procurement of Equipment: Purchase Cellebrite products (Inseyets and Guardian) and the new UPS.
Training Execution:
Enrollment: Enroll selected members in the training courses.
Training Sessions: Members attend and complete the training as scheduled.
Skill Application: Apply the learned skills to enhance cybersecurity practices at the Cyber Center.
Equipment Deployment:
Cellebrite Products:
Installation and Setup: Set up Inseyets and Guardian.
Utilization: Use these tools for digital forensics and evidence management.
UPS Replacement:
Installation by IT Technicians: Replace the old UPS with the new one.
Testing and Validation: Ensure the new UPS is functioning correctly and providing reliable power to the primary server.
Continuous Monitoring and Assessment: Use the newly acquired skills and tools to monitor, audit, and mitigate cybersecurity risks continuously.
By following this detailed process and involving qualified personnel at each step, the project will significantly enhance the Northern Nevada Cyber Center's ability to respond to and manage cybersecurity threats.

8. Describe, in a few sentences, the desired outcome(s) of your project.
Provide training and equipment to personnel in the Northern Nevada Cyber Center that ensures they are appropriately trained and equipped for cybersecurity issues, commensurate with their responsibilities as law enforcement officers in northern Nevada. Improve our processes to assess cybersecurity vulnerabilities and mitigate threats to our cyber center. Enhance the cyber center's preparation and resilience against cybersecurity risks and threats. Increase our abilities to assist and support government entities in northern Nevada in preventing and responding to cybersecurity incidents.

% of rural communities served.
The Northern Nevada Cybercenter serves communities in the northern half of Nevada, including but not limited to: Washoe, Carson, Douglas, Lyon, Humboldt, Pershing, Churchill, Mineral, Lander, Elko, Eureka, White Pine, and the northern part of Nye County. Apart from Reno, Sparks, and Carson City, all cities in these areas have a population of less than 50,000 and are considered rural and include tribal territories. Towns/cities in these areas include, but are not limited to: Fallon, Lovelock, Winnemucca, Battle Mountain, Eureka, Elko, Carlin, Wells, West Wendover, and Ely. Geographically, over 90% of the area we serve are rural. Approximately 50% of DEM funding supports the services for these areas.

9. Management & Administration (M&A) costs are not being awarded for this grant, per the Governor's Cybersecurity Task Force. Please indicate your understanding.
M&A costs are not operational costs but are necessary costs incurred in direct support of the grant, or as a consequence of the grant (i.e., financial management, reporting, oversight of those involved in the operational aspects of the grant)
NA

10. Does this project require new construction, renovation, retrofitting, or modifications of an existing structure which would necessitate an Environmental Planning and Historic Preservation (EHP) review?
EHP reviews are required for ANY project that disrupts the environment or a structure, including small things like putting nails in walls. Projects which require an EHP are unallowable under SLCGP.
- ☐ Yes
- ☑ No

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), either on our own or as a condition of FY 2022 SLCGP
- ☐ 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. 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.
This project is scalable, with various components that can be reduced or expanded based on resources, threats, and needs.
Ways to Reduce the Project:
Training Scope - Train key staff only, reducing frequency and focusing on essential modules.
Equipment Procurement - Selectively purchase critical tools and spread acquisition over time.
Ways to Expand the Project:
Enhanced Training - Provide comprehensive training to all personnel with regular refreshers.
Advanced Equipment - Acquire a full range of tools and the latest cybersecurity technologies.
Reasons for Scalability:
Resource Availability - Adjust based on budget and funding.
Threat Landscape - Evolve focus to address emerging threats.
Technological Advancements - Integrate new technologies.
Operational Needs - Tailor to specific needs of cyber center and the community.
This scalability ensures the project can dynamically adjust to changing circumstances, effectively combating cybersecurity threats.

13. Provide the 5-digit zip code where the project will be executed.
The project location could be different than the sub-recipient address.
89512

14. 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

15. 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

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

Each selection should have an accompanying item in the line item detail budget table on the next tab

- ☐ 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

Line Item Detail Budget *top*

PLANNING COSTS

Planning Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
				$		
		0	**0.00**	$ 0.00		

ORGANIZATION COSTS

Organizational Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
			$	$		
		0	**$ 0.00**	$ 0.00		

EQUIPMENT COSTS

Equipment Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase (s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	AEL Name - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info	AEL Number - Search https://www.fema.gov/grants/tools/authorized-equipment-list to find AEL info
Cellebrite - Inseyets/Guardian or product with same capabilities	7 Inseyets Licenses - ($7,829.57/License - Total = $54,806.99), 150 Inseyets Unlocks - ($217.50/Unlock - Total = $32,625.00), 7 Guardian Licenses ($10,159.79/License - Total = $71,118.53)	1	$ 158,550.52	$ 158,550.52	2. Monitor, audit, and track network traffic and activity: • Cellebrite Software: Allows the Cyber Center to monitor, audit, and track digital devices and activity, ensuring comprehensive oversight of network traffic and user activities.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	Software, Forensic	05HS-00-FRNS

					3. Enhance preparation, response, and resilience: • Training Courses: Equip personnel with skills to respond to cybersecurity threats. • Cellebrite Software and UPS Replacement: Improve system resilience and response capabilities.			
Liebert EXS UPS or product with same capabilities	One (1) Liebert EXS, Model 53S30HCFR0CB0SW, 30 kVA / 30 kW Capacity, 3 phase UPS with 2 String(s)	1	$ 40,000.00	$ 40,000.00	3. Enhance preparation, response, and resilience: • Training Courses: Equip personnel with skills to respond to cybersecurity threats. • Cellebrite Software and UPS Replacement: Improve system resilience and response capabilities.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	Components, Networking, D	04HW-03-NETD
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
			$	$				
		2	**$ 198,550.52**	$ 198,550.52				

TRAINING COSTS

Training Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this training with the State Training Officer?
1 - Training Course Registration	Practical Open-Source Intelligence (OSINT) - (Registration $8,525 x3, GOSI Certification $979 x3)	1	$ 28,512.00	$ 28,512.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
1 - Training Course Travel	San Diego, Start May 5, 2025 - Airfare ($450 x3 = $1,350), Lodging ($194 x6 Nights x3 = $3,492), M&IE 5 Days ($74 + 2 Travel Days @ $55.50 x 3 People = $1,443), Misc Travel $194 x6 Nights x3 People x +15% (approx) = $525	1	$ 6,810.00	$ 6,810.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
2 - Training Coure Registration	Performing a Cybersecurity Risk Assessment - On Demand - (Registration $3,405)	1	$ 3,405.00	$ 3,405.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
3 - Training Course Registration	Foundations: Computers, Technology, & Security - Web-Based - (Registration $3,020 x2, GFACT Certification $380 x2)	1	$ 6,800.00	$ 6,800.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
4 - Training Course Registration	Introduction to Cyber Security - On Demand - (Registration $7,430, GSIF Certification $979)	1	$ 8,409.00	$ 8,409.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue	NO

					threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Generation Strategies	
5 - Training Course Registration	Reverse-Engineering Malware: Malware Analysis Tools and Techniques - (Registration $8,525 x2, GREM Certification $979 x3)	1	$ 28,512.00	$ 28,512.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
5 - Training Course Travel	Las Vegas, Start Sep 4, 2024 - Airfare ($450 x3 = $1,350), Lodging ($194 x6 Nights x3 = $3,492), M&IE 5 Days ($74 + 2 Travel Days @ $55.50 x 3 People = $1,443), Misc Travel $194 x6 Nights x3 People x +15% (approx) = $525	1	$ 6,810.00	$ 6,810.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
6 - Training Course Registration	Security Essentials - Network, Endpoint, and Cloud - On Demand - (Registration $8,525, GSEC Certification $979)	1	$ 9,504.00	$ 9,504.00	Training Courses equip personnel with skills to respond to cybersecurity threats. Training and Equipment Updates: Ensure alignment between IT and operational technology cybersecurity objectives. Training in Risk Assessment (LDR419) helps the manager implement continuous vulnerability assessments. Ensures personnel are updated on the latest threat mitigation practices. Comprehensive Training Programs address gaps in knowledge, skills, and abilities, following the NICE Framework to improve the cybersecurity workforce.	Budget Allocation within Participating Agencies, Grant Renewal or Extension, Partnerships and Collaborations, Revenue Generation Strategies	NO
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		8	**$ 98,762.00**	$ 98,762.00			**0**

EXERCISE COSTS

Exercise Cost Name	Line Item Description	Quantity	Unit Cost	Total	Describe how the purchase(s) within this element tie into the project as described in the Application Questions section.	How would your organization sustain this project if grant funding was reduced or discontinued?	Do you plan to coordinate this exercise with the State Exercise Officer?
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
			$	$			
		0	**$ 0.00**	$ 0.00			**0**
Total		**0**	**$ 0.00**	$0.00			**0**

Document Uploads *top*

Documents Requested *	Required?	Attached Documents *
A-133 Audit (Most Current)	☑	A-133 Audit FY2023
Travel Policy	☑	WC Travel Policy
Payroll Policy	☑	Payroll Policy
Procurement Policy	☑	Procurement Policy
Milestones download template	☑	Project Milestones

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

Application ID: 481505

Outlook

RE: FY 2023 SLCGP - Northern Nevada Cyber Center Project

From Van Der Wall, Sam <svanderwall@washoecounty.gov>
Date Fri 09/27/24 11:32 AM
To DiMaggio, Rebecca <RDimaggio@washoecounty.gov>; Amanda Jackson <amanda.jackson@dem.nv.gov>

Hello Amanda,

Build or Sustain: The question asked me to select either "build" or "sustain," though this project actually involves both. I chose "sustain" because key aspects of the project, like maintaining our core capabilities with Cellebrite software, fall under this category. However, it is important to note that the project also includes elements of "build." For instance, the training component will expand our capabilities in cybersecurity, risk assessment, and open-source intelligence. Additionally, while the Cellebrite software licenses will help sustain our current capabilities, the company has mandated a transition to upgraded products within the year, meaning we're also preparing for necessary future upgrades. The replacement of the UPS will restore previous functionality, but since the current UPS is completely non-functional, it will also introduce new capabilities. Therefore, though I selected "sustain," the project clearly addresses both build and sustainment needs.

Please let me know if you need additional information.

Samuel Van Der Wall, Detective Sergeant
Washoe County Sheriff's Office
Internet Crimes Against Children (ICAC)
Regional Sex Offender Notification Unit (RSONU)
Human Exploitation and Recovery Operations (HERO)
Hostage Negotiations Team (HNT)
911 Parr Blvd, Reno, NV 89512
Desk: (775) 328-3048
svanderwall@washoecounty.gov

From: DiMaggio, Rebecca <RDimaggio@washoecounty.gov>
Sent: Thursday, September 26, 2024 3:14 PM
To: Amanda Jackson <amanda.jackson@dem.nv.gov>; Van Der Wall, Sam <svanderwall@washoecounty.gov>
Subject: FW: FY 2023 SLCGP - Northern Nevada Cyber Center Project

Hi Amanda,

Sam could you answer Amanda's question? I'm leaving soon and am off tomorrow.

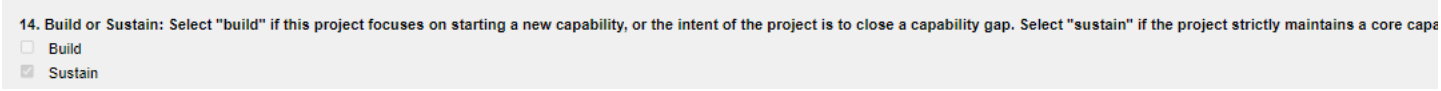
I think it might be an interpretation of build vs sustain.

Rebecca DiMaggio
Grants Coordinator
911 Parr Blvd. Reno, NV 89512
Tel: 775-328-3013 ● M-F 7 am-3 pm
Email: rdimaggio@washoecounty.gov
Grants: SOgrants@washoecounty.gov
Web: www.WashoeSheriff.com

From: Amanda Jackson <amanda.jackson@dem.nv.gov>
Sent: Thursday, September 26, 2024 2:59 PM
To: DiMaggio, Rebecca <RDimaggio@washoecounty.gov>
Cc: SOGrants <SOGrants@washoecounty.gov>; DHSGrants <DHSGrants@dem.nv.gov>
Subject: Re: FY 2023 SLCGP - Northern Nevada Cyber Center Project

Hi Rebecca,

It looks great, and thank you for making those updates! I just have one more question that I forgot to ask in my last email. I noticed that Sam had put "Sustain" instead of "Build" as his response to Application Question 14.



Can you provide some information on why "Sustain" was selected if this is the first time this project will have been funded with SLCGP? Was a similar project funded with another one of the DEM-administered grants in the past?

Thank you!

Amanda Jackson

Grants & Projects Analyst II, Southern Nevada

Office Hours: Mon-Fri, 7:00am-4:00pm

Nevada Division of Emergency Management / Homeland Security

Prevent • Protect • Mitigate • Respond • Recover

4500 W Silverado Ranch Blvd

Las Vegas, NV 89139

775-546-8055

775-687-0498 - 24/7/365 Emergency Duty

Book time to meet with me

Make sure you receive all DEM grants communication! Email DHSgrants@dem.nv.gov to be added to the grants listserv.

http://dem.nv.gov

From: DiMaggio, Rebecca <RDimaggio@washoecounty.gov>
Sent: Thursday, September 26, 2024 10:29 AM
To: Amanda Jackson <amanda.jackson@dem.nv.gov>
Subject: RE: FY 2023 SLCGP - Northern Nevada Cyber Center Project

Ok, everything is updated.

Rebecca DiMaggio
Grants Coordinator
911 Parr Blvd. Reno, NV 89512
Tel: 775-328-3013 ● M-F 7 am-3 pm
Email: rdimaggio@washoecounty.gov
Grants: SOgrants@washoecounty.gov
Web: www.WashoeSheriff.com

From: Amanda Jackson <amanda.jackson@dem.nv.gov>
Sent: Thursday, September 26, 2024 8:10 AM
To: DiMaggio, Rebecca <RDimaggio@washoecounty.gov>
Subject: Re: FY 2023 SLCGP - Northern Nevada Cyber Center Project

	Applicant Name	Rebecca Dimaggio
	Project Name:	Northern Nevada Cyber Center
	Project Funding Stream:	FY 2023 SLCGP
	Milestone Description*	Date of Expected Completion
1	BCC Approval - Receive BCC approval to utilize grant funds by October 1, 2024.	October 1 2024
2	Equipment/Hardware - Purchase and install replacement UPS for main cyber center server by November 1, 2024.	November 1 2024
3	Equipment/Software - Renew/Upgrade Cellebrite software - 7 Inseyets License, 150 Inseyets Unlocks, 7 Guardian Licenses by June 8, 2025.	June 8 2025
4	Training - Identify training needs; develop training; deliver training; and evaluate training by October 1, 2026.	October 1 2026
5	Close Out	End of Project
6		
7		
8		
9		
10		

*Please add additional rows as necessary for your project